ON THE NÉRON-SEVERI GROUPS OF FIBERED VARIETIES

SIMAN WONG February 1, 2008 – 07 : 29 **DRAFT**

Abstract. We apply Tate's conjecture on algebraic cycles to study the Néron-Severi groups of varieties fibered over a curve. This is inspired by the work of Rosen and Silverman, who carry out such an analysis to derive a formula for the rank of the group of sections of an elliptic surface. For a semistable fibered surface, under Tate's conjecture we derive a formula for the rank of the group of sections of the associated Jacobian fibration. For fiber powers of a semistable elliptic fibration $\mathcal{E}\to C$, under Tate's conjecture we give a recursive formula for the rank of the Néron-Severi groups of these fiber powers. For fiber squares, we construct unconditionally a set of independent elements in the Néron-Severi groups. When $\mathcal{E}\to C$ is the universal elliptic curve over the modular curve $X_0(M)/\mathbf{Q}$, we apply the Selberg trace formula to verify our recursive formula in the case of fiber squares. This gives an analytic proof of Tate's conjecture for such fiber squares over $\mathbf{Q}$, and it shows that the independent elements we constructed in fact form a basis of the Néron-Severi groups. This is the fiber square analog of the Shioda-Tate Theorem.

Contents

1. Introduction

Let K be a field which is finitely generated over its prime field, and let A be an Abelian variety defined over K. The Mordell-Weil Theorem [9, p. 138] shows that $A(K)$ is a finitely generated Abelian group. It is of great number-theoretic interest to determine the rank of $A(K)$. If K is a global field, the Birch-Swinnerton-Dyer conjecture (as generalized by Tate [28]) predicts that the Hasse-Weil L-function $L(A/K,s)$ of A/K has an analytic continuation to the whole complex plane, and that it has a zero at $s=1$ of order equal to the rank of

Key words and phrases. Elliptic curves over finite fields, elliptic surfaces, Kuga fiber varieties, modular forms, Néron-Severi groups, Selberg trace formula, Tate conjecture.

$A(K)$. This latter statement is equivalent to saying that the rank of $A(K)$ is equal to the residue at $s=1$ of the logarithmic derivative of $L(A/K,s)$. Now, take $K=\mathbf{Q}$ and A to be an elliptic curve E over $\mathbf{Q}$. A formal[1] Tauberian argument then leads Nagao [14] to observe that the expression

$$\frac{-1}{x}\sum_{p\leq x} a_p(E)\log p, \tag{1}$$

where $a_p(E) := p+1-\#(\text{non-singular points of } E \bmod p)$, approximates the rank of $E(\mathbf{Q})$ for suitable, large values of x. This is supported by computer data [12]. For an elliptic curve $\mathcal{E}$ defined over the rational function field $\mathbf{Q}(T)$, Nagao [14] defines a similar expression

$$S(\mathcal{E},x) := \frac{-1}{x}\sum_{p\leq x}\frac{1}{p}\sum_{t\in\mathbf{F}_p} a_p(\mathcal{E}_t)\log p, \tag{2}$$

where $\mathcal{E}_t$ denotes the curve obtained from $\mathcal{E}$ by specializing the variable T to t. For several families of elliptic curves $\mathcal{E}$ over $\mathbf{Q}(T)$, Nagao [14] shows that $S(\mathcal{E},x)$ converges to the Mordell-Weil rank of $\mathcal{E}$ over $\mathbf{Q}(T)$, and he conjectures that this is true in general:

$$\text{MW-rank } \mathcal{E}(\mathbf{Q}(T)) \overset{?}{=} \lim_{x\to\infty}\frac{-1}{x}\sum_{p\leq x}\frac{1}{p}\sum_{t\in\mathbf{F}_p} a_p(\mathcal{E}_t)\log p. \tag{3}$$

Elliptic curves over $\mathbf{Q}(T)$ can be viewed as elliptic surfaces over $\mathbf{P}^1_{\mathbf{Q}}$. More precisely, let C be a smooth, geometrically connected projective curve defined over a number field k; denote by $K_C = k(C)$ its function field. Let E be an elliptic curve over K_C. By the theory of minimal models [2], there exists a smooth projective surface $\mathcal{E}$ together with a genus one fibration $f : \mathcal{E}\to C$ with a section σ, all defined over k, such that the generic fiber of f is E/K_C, and that no fiber of f contains a curve $\simeq \mathbf{P}^1$ and with self-intersection number -1; such elliptic fibrations are called relatively minimal. Furthermore, the correspondence $E/K_C \leftrightarrow (\mathcal{E},f)$ is bijective [11]. Denote by $NS(\mathcal{E}/k)$ the Néron-Severi group of the surface $\mathcal{E}/k$. Fix an algebraic closure $\overline{k}$ of k, and write G_k for the absolute Galois group $\mathrm{Gal}(\overline{k}/k)$. Given a maximal ideal $\mathfrak{p}$ of the ring of integers $\mathcal{O}_k$ of k, denote by $N_{\mathfrak{p}}$ the absolute norm of $\mathfrak{p}$. For any smooth variety V/k of dimension >0, Tate's conjecture on algebraic cycles [27] states that $L_2(V/k,s)$, the L-function attached to $H^2_{\text{ét}}(V\otimes\overline{k},\mathbf{Q}_l)$, has meromorphic continuation to $\mathbf{C}$, and that

$$NS(V/k)\otimes\mathbf{Q}_l \simeq H^2_{\text{ét}}(V\otimes\overline{k},\mathbf{Q}_l(1))^{G_k}, \tag{4}$$

$$-\operatorname*{ord}_{s=2} L_2(V/k,s) = \dim H^2_{\text{ét}}(V\otimes\overline{k},\mathbf{Q}_l(1))^{G_k}. \tag{5}$$

On the other hand, the Shioda-Tate formula [24] furnishes a natural isomorphism

$$E(\overline{k}(C)) \simeq NS(\mathcal{E}/\overline{k})/T_{\mathcal{E}}, \tag{6}$$

where $T_{\mathcal{E}}$ denotes the subgroup of $NS(\mathcal{E}/\overline{k})$ generated by the section σ together with all the $\overline{k}$-components of the fibers of f. This leads Silverman to consider the following analytic form of Nagao's conjecture

$$\text{MW-rank of } \mathcal{E}(k(C)) \overset{?}{=} \operatorname*{res}_{s=1}\sum_{\mathfrak{p}}\frac{-\log N_{\mathfrak{p}}}{N_{\mathfrak{p}}^{s+1}}\sum_{t\in C(\mathbf{F}_{\mathfrak{p}})} a_{\mathfrak{p}}(\mathcal{E}_t) \tag{7}$$

[1] the Tauberian theorem is not applicable since the $a_p(E)$'s change sign.

and asks if it is related to Tate's conjecture. By giving an L-series interpretation of the Shioda-Tate formula and by analyzing carefully the singular fibers of the elliptic surface $\mathcal{E}$, Rosen and Silverman [16] show that, for any non-split elliptic surface $f : \mathcal{E} \to C$ with a section, (7) indeed follows from Tate's conjecture. The original Nagao's conjecture then follows from (7) plus a non-vanishing hypothesis for $L_2(\mathcal{E}/\mathbf{Q}, s)$. In particular, Rosen and Silverman show that Nagao's conjecture holds unconditionally for rational elliptic surfaces with sections.

This result of Rosen and Silverman can be thought of as a Birch-Swinnerton-Dyer-type conjecture for *families* of elliptic curves over C/k. If $\mathcal{E}_t$ has good reduction at $\mathfrak{p}$, then $a_\mathfrak{p}(\mathcal{E}_t)$ is the trace of the geometric Frobenius at $\mathfrak{p}$ of $H^1_{\text{ét}}(C \otimes \overline{k}, \mathbf{Q}_l)$. A natural question then arises: are there analogs of Nagao's conjecture for general fibered varieties over a curve? In this paper we investigate this question for fibered surfaces and for fiber powers of elliptic fibrations.

Our first result gives an analog of the analytic form of Nagao's conjecture for higher genus fibrations (see Section 2 for the definition of Chow traces, and see Section 3 for the definition of $a_\mathfrak{p}(S_t)$). Note that the hypothesis on multiplicities in Theorem 1 is satisfied in the case of a semistable fibration, or if the fibration has a section.

Theorem 1. *Let S be a smooth projective surface, and let $\pi : S \to C$ be a fibration over a smooth projective curve C, all defined over a number field k. Suppose that for every point $x \in C(\overline{k})$, the GCD of the multiplicities of the irreducible components of the fiber $\pi^{-1}(x)$ is 1, and that the Chow trace of this fibration is zero. Assume Tate's conjecture for S/k. Then*

$$\underset{s=1}{res} \sum_{\mathfrak{p}} \frac{-\log N_\mathfrak{p}}{N_\mathfrak{p}^{s+1}} \sum_{t \in C(\mathbf{F}_\mathfrak{p})} a_\mathfrak{p}(S_t) \quad = \quad \begin{array}{l}\textit{the rank of the group of sections of the}\\ \textit{Jacobian fibration associated to } S \to C.\end{array}$$

Remark 1. For any integer $g \geq 1$ there exists a semistable, genus g fibration $X \to \mathbf{P}^1$ over some number field, such that X is a rational surface and that the Mordell-Weil rank of the Jacobian fibration is $4g + 4$; cf. [17] and [25]. Since Tate's conjecture is true for rational surfaces, this shows that Theorem 1 is not vacuous.

Next, consider the problem of studying Nagao sums for $a_\mathfrak{p}(\mathcal{E}_t)^n$ where $\mathcal{E} \to C$ is an elliptic fibration. Since $|a_\mathfrak{p}(\mathcal{E}_t)^n| \leq (4N_\mathfrak{p})^{n/2}$,

$$\text{(8)} \qquad \underset{s=1}{\text{res}} \sum_{\mathfrak{p}} \frac{-\log N_\mathfrak{p}}{N_\mathfrak{p}^{s+\lambda}} \sum_{t \in C(\mathbf{F}_\mathfrak{p})} a_\mathfrak{p}(\mathcal{E}_t)^n = 0 \qquad \text{for every real number } \lambda > n/2 + 1.$$

It is then natural to try to compute the residue at $\lambda = n/2 + 1$, and to ask if there is any geometric interpretations of these residues at every integer $\geq n/2 + 1$. To state our results, first note that the relation $a_\mathfrak{p}(\mathcal{E}_t) = p + 1 - \#\mathcal{E}_t(\mathbf{F}_\mathfrak{p})$ suggests that the Nagao sum for $a_\mathfrak{p}(\mathcal{E}_t)^n$ should be related to

$$\mathcal{E}^{(n)} := \text{the fiber product of } n \text{ copies of } \mathcal{E} \text{ with itself over } C.$$

Indeed, let $f : \mathcal{E} \to C$ be a semistable elliptic fibration over a number field k. Deligne ([3]; cf. also [19]) constructs a desingularization $\tilde{\mathcal{E}}^{(n)}$ of $\mathcal{E}^{(n)}$ via a canonical sequence of blowups.

Set $b_j :=$ the number of k-rational exceptional divisors of $\widetilde{\mathcal{E}}^{(j)}$. Since $\widetilde{\mathcal{E}}^{(1)} = \mathcal{E}$ is smooth, we have $b_1 = 0$. For $\mathcal{E}^{(2)}$ the singular locus consists of finitely many ordinary double points.

Theorem 2. *Let $f : \mathcal{E} \rightarrow C$ be a semistable elliptic fibration over k with a section. Fix an integer $n \geq 2$. Assume Tate's conjecture for $\widetilde{\mathcal{E}}^{(j)}$ for every $1 \leq j \leq n$. Then*

$$\underset{s=1}{res} \sum_{\mathfrak{p}} \frac{-\log N_{\mathfrak{p}}}{N_{\mathfrak{p}}^{s+n}} \sum_{t \in C(\mathbf{F}_{\mathfrak{p}})} a_{\mathfrak{p}}(\mathcal{E}_t)^n \;=\; -1 + \sum_{j=1}^{n} (-1)^j \binom{n}{j} \cdot (b_j - \textit{rank } NS(\widetilde{\mathcal{E}}^{(j)}/k)). \tag{9}$$

Remark 2. Note that the left side of (9) makes no reference to any desingularization of $\mathcal{E}^{(n)}$, and that in general $\mathcal{E}^{(n)}$ has many desingularizations. For example, every the ordinary double point on $\mathcal{E}^{(2)}/\overline{k}$ admits a small resolution [4, Example IV-29]. This process replaces each ordinary double point by a $\mathbf{P}^1$ instead of $\mathbf{P}^1 \times \mathbf{P}^1$ (as in the case of blowup) and is an isomorphism outside the double points. In particular, it does not affect the Néron-Severi group. On the other hand, when we evaluate the residue (9) unconditionally in the case of elliptic modular surfaces (Theorem 4), we need to work with Deligne's canonical desingularization in order to relate the threefold $\widetilde{\mathcal{E}_M}^{(2)}$ to modular forms.

Let us examine the case $n = 2$ of this Theorem in greater details. Since $a_{\mathfrak{p}}(\mathcal{E}_t)^2 \leq 4N_{\mathfrak{p}}$, when $n = 2$ the residue in (9) is between -4 and 0. Theorem 2 then suggests that the rank of $NS(\widetilde{\mathcal{E}}^{(2)}/k)$ is equal to

$$2 \text{ rank } NS(\mathcal{E}/k) + (\#k\text{-rational singular points of } \mathcal{E}^{(2)}) - 1 - S_{\mathcal{E}},$$

where $S_{\mathcal{E}} \in \{0, -1, -2, -3, -4\}$. On the other hand, there is a natural collection of divisors on $\widetilde{\mathcal{E}}^{(2)}$ obtained by essentially pulling back to $\widetilde{\mathcal{E}}^{(2)}$, via the two projections $\mathcal{E}^{(2)} \rightarrow \mathcal{E}$, the generators of $NS(\mathcal{E}/k) \otimes \mathbf{Q}_l$ furnished by the Shioda-Tate Theorem; cf. the list (29) in §5 for details. The cardinality of this natural collection of divisors is (cf. (30))

$$2 \text{ rank } NS(\mathcal{E}/k) + (\#k\text{-rational singular points of } \mathcal{E}^{(2)}).$$

In light of Theorem 2, if these divisors form a basis of $NS(\widetilde{\mathcal{E}}^{(2)}/k) \otimes \mathbf{Q}$, then the residue in (9) would be exactly -1 when $n = 2$. We have the following partial result.

Theorem 3. *Let $f : \mathcal{E} \rightarrow C$ be a semistable elliptic fibration over k with a section. Then the divisors in* (29) *on $\widetilde{\mathcal{E}}^{(2)}$ give rise to independent elements in $NS(\widetilde{\mathcal{E}}^{(2)}/k) \otimes \mathbf{Q}$.*

Corollary 1. *Let $f : \mathcal{E} \rightarrow C$ be a semistable elliptic fibration over k with a section. Assume Tate's conjecture for $\mathcal{E}$ and $\widetilde{\mathcal{E}}^{(2)}$. Then*

$$\underset{s=1}{res} \sum_{\mathfrak{p}} \frac{-\log N_{\mathfrak{p}}}{N_{\mathfrak{p}}^{s+2}} \sum_{t \in C(\mathbf{F}_{\mathfrak{p}})} a_{\mathfrak{p}}(\mathcal{E}_t)^2 < 0. \tag{10}$$

Remark 3. Let $f : \mathcal{E} \rightarrow C$ be a semistable fibration over k with a section. Suppose that every $\overline{k}$-irreducible component of the bad fibers is defined over k. Let Γ be such a component, and set $\gamma := f(\Gamma) \in C$, so the fiber $f^{-1}(\gamma)$ is a m-gon for some $m \geq 1$. The fiber above γ in the singular threefold $\mathcal{E}^{(2)} \rightarrow C$ then consists of m^2 divisors. After blowing up the m^2 ordinary double points, we pick up m^2 exceptional divisors along with the original m^2 divisors on $\widetilde{\mathcal{E}}^{(2)}$, all Cartier.[2] In light of Theorems 3 and 2, we see that Tate's conjecture implies that only about half of these divisors are independent in $NS(\widetilde{\mathcal{E}}^{(2)}/k)$. What are these divisorial relations?

The residue in (10) encodes in analytic terms an equidistribution statement for the traces of Frobenius for the fibers of an elliptic surface: To say that the residue is zero is to say that most of the fibers have small $a_{\mathfrak{p}}$, while to say that the residue is -4 is to say that most of the fibers have $a_{\mathfrak{p}}$ close to the extremal values $\pm 2\sqrt{N_{\mathfrak{p}}}$. We can pose the same problem for elliptic curves over number fields; as usual we get the strongest results in the context of modular elliptic curves over $\mathbf{Q}$, for which analytic techniques are available. Similarly, in the important case of elliptic modular surfaces, by relating the $a_p(\mathcal{E}_t)^n$-sum to the Selberg trace formula we prove the following result.

Theorem 4. *Fix an odd, positive integer M. Denote by $f_M : \mathcal{E} \rightarrow X_0(M)$ the elliptic modular surface over $\mathbf{Q}$ associated to the modular curve $X_0(M)$. For every integer $n \geq 2$, denote by $[n/2]$ the largest integer $\leq n/2$. Then the series*

$$\sum_p \frac{-\log p}{p^{s+[n/2]+1}} \sum_{t \in X_0(M)(\mathbf{F}_p)} a_p(\mathcal{E}_t)^n$$

has a meromorphic continuation to the half plane $Re(s) > 0$ with at most a simple pole at $s = 1$. The pole occurs precisely when n is even, in which case the residue is $\dfrac{-(n!)}{(n/2)!(n/2+1)!}$.

Remark 4. (a) Since $|a_p(\mathcal{E}_t)^n| \leq 2^n p^{n/2}$, a trivial lower bound of the residue in Theorem 4 is $\geq -2^n$. But the Stirling formula gives

$$\frac{n!}{(n/2)!(n/2+1)!} = \frac{2^n}{(n/2)^{3/2}} \frac{e^{O(1/n)}}{e^4\sqrt{2\pi}},$$

which is $o(2^n)$. Thus on average, $|a_p(\mathcal{E}_t)|$ is 'small'.

(b) For odd n, Theorem 4 is stronger than (8) in that it gives the residue at a point to the *left* of the trivial boundary of convergence. Furthermore, for odd n, our argument in fact holds over all number fields. However, for even n our use of the Selberg trace formula forces us to work over $\mathbf{Q}$. If we can directly relate, say, expression (39) to counting points on Kuga fiber varieties without using the trace formula then we should be able to work with arbitrary base fields.

(c) The requirement that M be odd is a simplifying assumption; with additional (tedious) work the Theorem should hold for general M.

As a by-product of Theorem 4, we get an analytic proof of Tate's conjecture for the universal elliptic curve $\mathcal{E}_M \rightarrow X_0(M)/\mathbf{Q}$ and for its fiber square.

[2] Denote by $\mathring{\mathcal{E}}^{(2)}$ the complement of the ordinary double points in $\mathcal{E}^{(2)}$. Then the m^2 Weil divisors on $\mathcal{E}^{(2)}$ also give rise to m^2 divisors $\{W_i\}_i$ on $\mathring{\mathcal{E}}^{(2)}$. These are now Cartier divisors since $\mathring{\mathcal{E}}^{(2)}$ is smooth. The Zariski closure in $\widetilde{\mathcal{E}}^{(2)}$ of the W_i then give rise to m^2 Cartier divisors on $\widetilde{\mathcal{E}}^{(2)}$.

Theorem 5. *Let M be an odd integer.*

(i) *The L-functions $L_2(\mathcal{E}_M/\mathbf{Q}, s)$ and $L_2(\widetilde{\mathcal{E}_M}^{(2)}/\mathbf{Q}, s)$ associated to the elliptic modular surface $\mathcal{E}_M \to X_0(M)$ over $\mathbf{Q}$ has an analytic continuation to $Re(s) > 7/4$ except for a pole at $s = 2$ of order equal to $rank NS(\mathcal{E}_M/\mathbf{Q})$ and $rank NS(\widetilde{\mathcal{E}_M}^{(2)}/\mathbf{Q})$, respectively. In addition, Tate's conjecture holds for $\mathcal{E}_M/\mathbf{Q}$ and for $\widetilde{\mathcal{E}_M}^{(2)}/\mathbf{Q}$.*

(ii) *The collection of divisors in* (29) *gives rise to a basis of $NS(\widetilde{\mathcal{E}_M}^{(2)}/\mathbf{Q}) \otimes \mathbf{Q}$.*

Remark 5. (a) For Kuga fiber varieties over the full congruence subgroup $\Gamma(N)$, the first part of Tate's conjecture (4) has been verified [5]; the argument there is most likely to be applicable for $\mathcal{E}_M$ as well. The second part of Tate's conjecture (5) is probably known to the experts for such Kuga varieties too (cf. Remark 15 in Section 8), but we have not been able to locate a proof in the literature.

(b) Theorem 5(ii) is the fiber-square analog of the Shioda-Tate Theorem for $\mathcal{E}_M \to X_0(M)/\mathbf{Q}$; cf. Theorem 8 below.

Remark 6. Our method can be applied to study higher fiber powers of $\mathcal{E}_M \to X_0(M)$. To do that we need an analog of Theorem 3 for such higher fiber powers. That calls for a careful accounting of the pull-back divisors obtained via various projections $\widetilde{\mathcal{E}}^{(j)} \to \mathcal{E}$, together with a detail analysis of the exceptional divisors arised from Deligne's canonical desingularization. Such an analysis is also needed if we want to apply our techniques to study the groups of d-cycles on $\widetilde{\mathcal{E}}^{(j)}$ modulo l-adic homological equivalence for $0 < d < n$ (for $d = n - 1$ we recover the Néron-Severi group). We will address these issues in a separate paper.

Remark 7. Our method yields no information regarding the torsion subgroups of the Néron-Severi groups of fibered varieties. For example, are there any additional torsion divisors on $\widetilde{\mathcal{E}}^{(j)}$ other than the pull-back of torsion divisors on $\mathcal{E}$? Do non-trivial torsion divisors on $\mathcal{E}$ pull-back to non-trivial torsion divisors on $\widetilde{\mathcal{E}}^{(j)}$?

Remark 8. Using the computer algebra package PARI, we evaluate numerically the a_p^2-Nagao residues for several semistable elliptic fibrations which are not Kuga varieties. In each case our data strongly suggests that the residue should be -1. In light of the spectral sequence computation in Section 8, to settle this question for a general semistable elliptic fibration $f : \mathcal{E} \to C$ we need to understanding the L-function attached to the l-adic monodromy representation $H^1_{\text{ét}}(C/\overline{k}, R^1 f_* \mathbf{Q}_l)$. In general this is very difficult problem. Currently, our effort is focused on the semistable elliptic surface $y^2 = x(x - A^{2n})(x + B^{2n})$ associated to the Fermat curve $A^{2n} + B^{2n} = C^{2n}$. This turns out to be the 'universal elliptic curve' over the Fermat curve [23], the latter being viewed as a modular curve with respect to a non-congruence subgroup of $SL(2, \mathbf{Z})$. We expect that the complex multiplication structure on the Fermat curve will greatly facilitate the monodromy calculation.

Remark 9. Nagao sums can be formulated for varieties fibered over a base of dimension > 1 as well. To mimic our argument to this setup, among other things we need to relate the cohomology of the base to that of the fibered variety; cf. Lemma 1. Significant results along this line have been obtained in the Ph. D. dissertation of Wazir [30].

The discussion above focuses primarily on semistable fibrations. At the other end of the spectrum we have the isotrivial, non-split elliptic fibrations: these are non-split elliptic surfaces $\mathcal{E} \rightarrow C$ where the j-invariant of the generic fiber is an element of k.

Theorem 6. *Let $f : \mathcal{E} \rightarrow C$ be an isotrivial, non-split elliptic surface over $\mathbf{Q}$. Then*

$$\underset{s=1}{res} \sum_p \frac{-\log p}{p^{s+2}} \sum_{t \in C(\mathbf{F}_p)} a_p(\mathcal{E}_t)^2 = \begin{cases} 0 & \textit{if } \mathcal{E} \rightarrow C \textit{ is a cubic, quartic} \\ & \textit{or sextic twist family,} \\ -1 & \textit{otherwise.} \end{cases}$$

Remark 10. Is there a geometric interpretation of this residue, *à la* Theorems 3 and 5(b)?

1.1. **Summary.**

Here is a summary of the paper. In Section 2 we recall Raynaud's exact sequence and the Shioda-Tate Theorem for higher genus fibrations. These geometric data are applied in Sections 3 and 4 to derive formulae for the rank of various Néron-Severi groups; Tate's conjecture comes in when we rewrite the Nagao sums in terms of the logarithmic derivatives of L-functions. In Section 5 we produce a natural collection of divisors on $\widetilde{\mathcal{E}}^{(2)}$; to prove that they are independent in $NS(\widetilde{\mathcal{E}}^{(2)}/k) \otimes \mathbf{Q}$ we intersect these divisors on the threefold $\widetilde{\mathcal{E}}^{(2)}$ with various well-chosen surfaces, reducing the problem of checking independence to the case of surfaces. In Sections 6 and 7 we switch gears and count elliptic curves over finite fields with a given level structure and a fixed j-invariant. This allows us to rewrite, in the case of the universal elliptic curve $\widetilde{\mathcal{E}_M}$ over $X_0(M)/\mathbf{Q}$, the a_p^n-Nagao sums in terms of the Selberg trace formula, from which Theorem 5 follows. Combined with a spectral sequence calculation, this yields an analytic proof of Tate's conjecture for $\widetilde{\mathcal{E}_M}^{(2)}$. Finally, in Section 9 we compute the a_p^2-Nagao residue for isotrivial fibrations over $\mathbf{Q}$, by relating these Nagao sums to symmetric square L-functions.

Convention. We will have many occasions to reduce a fibered variety $f : V \rightarrow C$ modulo a prime ideal $\mathfrak{p}$. Unless otherwise stated, the reduction is taken with respect to some fixed but possibly non-canonical model of the fibration. This introduces ambiguity for finitely many $\mathfrak{p}$, which does not affect our computation of the residues of various L-functions associated to V. In a similar vein, we adopt the convention of using only those $\mathfrak{p}$ at which V, C and f all have good reduction with respect to some fixed model; some fibers of course could be singular.

2. Raynaud's exact sequence and the Shioda-Tate formula

In this section we recall several results about fibered surfaces; see [26] for more details.

Let C be a smooth projective curve over k, and let S be a smooth projective surface over k. Denote by $Jac_k(C)$ the Jacobian variety of C/k, and by $\mathrm{PicVar}_s(S)$ the Picard variety of S/k; both of these are Abelian varieties over k. Let $\pi : S \rightarrow C$ be a proper morphism over k. Assume that the generic fibration of π is a smooth projective curve Γ_π over the function field $k(C)$. This gives rise to a short exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Pic}^0_{C/k} \arrow[r, "\pi^*"] \arrow[d, equal] & \mathrm{Pic}^0_{S/k} \arrow[r] \arrow[d, equal] & \mathrm{Pic}^0_{S/C}, \\
 & \mathrm{Jac}_k(C) & \mathrm{PicVar}_k(S) &
\end{tikzcd}$$

where $\mathrm{Pic}_{S/C}$ denotes the relative Picard scheme of S/C [2]. To identify the image of π^* we need the notion of Chow trace: let A be an Abelian variety over the function field $K_C := k(C)$. The *Chow trace* of A/K_C, denoted by $Tr_{K_C/k}(A)$, is an Abelian variety over k together with a K_C-homomorphism $\tau : Tr_{K_C/k}(A) \rightarrow A$, such that for any Abelian variety B/k and a K_C-homomorphism $\beta : B \rightarrow A$, there exists a unique k-homomorphism $\beta' : Tr_{K_C/k}(A) \rightarrow B$ such that $\beta = \tau \circ \beta'$ (cf. [9, p. 138]). Note that if $f : \mathcal{E} \rightarrow C$ is a genus one fibration, then f is non-split if and only if the Chow trace of $\mathcal{E} \rightarrow C$ is zero.

We say that $\pi : S \rightarrow C$ is a *Raynaud fibration* if for every fiber of π over $\overline{k}$, the GCD of the multiplicities of the irreducible components is 1. Two notable examples of Raynaud fibrations are (a) fibrations $S \rightarrow C$ with a section, and (b) semistable fibrations.

Theorem 7 (Raynaud [26, Thm. 2])**.** *Suppose $\pi : S \rightarrow C$ is a Raynaud fibration over k. Then we have a short exact sequence of Abelian varieties over k*

$$0 \rightarrow Jac_k(C) \overset{\pi^*}{\rightarrow} PicVar_k(S) \rightarrow Tr_{K_C/k}(Jac_{K_C}(\Gamma_\pi)) \rightarrow 0. \tag{11}$$

Corollary 2. *Suppose $\pi : S \rightarrow C$ is a Raynaud fibration over k with zero Chow trace. Then for all but finitely many $\mathfrak{p}$,*

$$trace(Frob_{\mathfrak{p}}, H^i_{\acute{e}t}(S \otimes \overline{k}, \mathbf{Q}_l)) = trace(Frob_{\mathfrak{p}}, H^i_{\acute{e}t}(C \otimes \overline{k}, \mathbf{Q}_l)). \tag{12}$$

Fix a smooth curve σ/k on S such that $\pi(\sigma) = C$. Fix a fiber $F/\overline{k}$ of π. Denote by T_S the subspace of $NS(S/\overline{k}) \otimes \mathbf{Q}$ generated by σ together with all components of all fibers of π over $\overline{k}$. While σ need not be a section of π, the image in $NS(S/\overline{k}) \otimes \mathbf{Q}$ of any two choices of σ differs by a $\mathbf{Q}$-multiple. In particular, T_S is well-defined.

Theorem 8 (Shioda-Tate [26])**.** *Suppose $\pi : S \rightarrow C$ is a Raynaud fibration over k with zero Chow trace. Then there is a decomposition of $\mathbf{Q}[G_k]$-modules*

$$NS(S/\overline{k}) \otimes \mathbf{Q} \simeq \big(Jac_{K_C\overline{k}}(\Gamma_\pi) \otimes \mathbf{Q}\big) \oplus T_S. \tag{13}$$

3. Nagao's conjecture for higher genus fibrations

Proof of Theorem 1. For any reduced, irreducible projective curve $X/\mathbf{F}_{\mathfrak{p}}$, not necessarily smooth, define

$$a_{\mathfrak{p}}(X) := N_{\mathfrak{p}} + 1 - \#X(\mathbf{F}_{\mathfrak{p}}).$$

Let $\pi : S \rightarrow C$ be a fibration of smooth projective surface over a smooth projective curve, all defined over a number field k. Suppose the fibration has good reduction[3] at $\mathfrak{p}$. For any $t \in C(\mathbf{F}_{\mathfrak{p}})$, write S_t for the fiber of π at t. Define

$$m(S_t/\mathbf{F}_{\mathfrak{p}}) := \text{number of reduced } \mathbf{F}_{\mathfrak{p}}\text{-rational components of the fiber } S_t.$$

[3] recall our convention

Denote by $\{C_i\}_i$ the $\mathbf{F}_\mathfrak{p}$-components of the fiber S_t. Define

$$a_\mathfrak{p}(S_t) := \sum_i a_\mathfrak{p}(C_i) + \sum_{x \in S_t(\mathbf{F}_\mathfrak{p})} \big[(\text{number of } C_i \text{ passing through } x) - 1\big] - \big[m(S_t/\mathbf{F}_\mathfrak{p}) - 1\big].$$

Note that $a_\mathfrak{p}(S_t)$ coincides with the usual definition when S is a genus one fibration (this follows from the case-by-case analysis in [16, Lem. 17]), or when S_t is a smooth fiber (in which case $a_\mathfrak{p}(S_t)$ is the trace of the geometric Frobenius at $\mathfrak{p}$ acting on $H^1_{\text{ét}}(S_t \otimes \overline{k}, \mathbf{Q}_l)$). Moreover, for every $t \in C(\mathbf{F}_\mathfrak{p})$, we have[4]

$$\#S_t(\mathbf{F}_\mathfrak{p}) = 1 - a_\mathfrak{p}(S_t) + N_\mathfrak{p} + (m(S_t/\mathbf{F}_\mathfrak{p}) - 1)N_\mathfrak{p}, \tag{14}$$

which is the analog for our fibration of [16, Lem. 17]. Consequently,

$$\#S(\mathbf{F}_\mathfrak{p}) = (1 + N_\mathfrak{q})\#C(\mathbf{F}_\mathfrak{p}) + \sum_{t \in C(\mathbf{F}_\mathfrak{p})} a_\mathfrak{p}(S_t) + \sum_{t \in C(\mathbf{F}_\mathfrak{p})} (m(S_t/\mathbf{F}_\mathfrak{p}) - 1)N_\mathfrak{p}. \tag{15}$$

On the other hand, since S has good reduction at $\mathfrak{p}$, the Weil conjecture gives

$$\#S(\mathbf{F}_\mathfrak{p}) = \sum_{i=0}^{4} (-1)^i \text{trace}(\text{Frob}_\mathfrak{p}, H^i_{\text{ét}}(S \otimes \overline{k}, \mathbf{Q}_l)). \tag{16}$$

Combine (15) and (16) together with (12), we get

$$\sum_{t \in C(\mathbf{F}_\mathfrak{p})} a_\mathfrak{p}(S_t) = -\text{trace}(\text{Frob}_\mathfrak{p}, H^2_{\text{ét}}(S \otimes \overline{k}, \mathbf{Q}_l)) + 2N_\mathfrak{q} + \sum_{t \in C(\mathbf{F}_\mathfrak{p})} (m(S_t/\mathbf{F}_\mathfrak{p}) - 1)N_\mathfrak{p}$$

Recall that the submodule T_S of the G_k-module $NS(S/\overline{k}) \otimes \mathbf{Q}$ is generated by a fixed multisection σ/k on S along with all components of all fibers of π over $\overline{k}$. The geometric Frobenius $\text{Frob}_\mathfrak{p}$ fixes σ and acts non-trivially on any non-$\mathbf{F}_\mathfrak{p}$-rational components of each fiber of π. Furthermore, in light of the Weil conjecture, π has at least one smooth fiber over $\mathbf{F}_\mathfrak{p}$ for all but finitely many $\mathfrak{p}$, and the image in $NS(S/\overline{\mathbf{F}_\mathfrak{p}}) \otimes \mathbf{Q}$ of any two such multisections differ by a non-zero $\mathbf{Q}$-multiple. Consequently, for all but finitely many $\mathfrak{p}$,

$$\sum_{t \in C(\mathbf{F}_\mathfrak{p})} (m(S_t/\mathbf{F}_\mathfrak{p}) - 1)N_\mathfrak{p} = 2 + \text{trace}(\text{Frob}_\mathfrak{p}, T_S),$$

whence

$$\sum_{t \in C(\mathbf{F}_\mathfrak{p})} a_\mathfrak{p}(S_t) \quad = \quad -\text{trace}(\text{Frob}_\mathfrak{p}, H^2_{\text{ét}}(S \otimes \overline{k}, \mathbf{Q}_l)) + \text{trace}(\text{Frob}_\mathfrak{p}, T_S)N_\mathfrak{p}. \tag{17}$$

Denote by $L(T_S, s)$ the L-function associated to the G_k-module T_S. Following [16, p. 52], we have, for $Re(s) > 7/4$,

$$\frac{d}{ds} \log L(T_S, s) \quad = \quad \sum_\mathfrak{p} -\text{trace}(\text{Frob}_\mathfrak{p}, T_S) \frac{\log N_\mathfrak{p}}{N_\mathfrak{p}^{s-1}} + O(1), \tag{18}$$

$$\frac{d}{ds} \log L_2(S/k, s) \quad = \quad \sum_\mathfrak{p} -\text{trace}(\text{Frob}_\mathfrak{p}, H^2_{\text{ét}}(S \otimes \overline{k}, \mathbf{Q}_l)) \frac{\log N_\mathfrak{p}}{N_\mathfrak{p}^{s-1}} + O(1). \tag{19}$$

[4] our definition of $a_\mathfrak{p}$ makes sense even if $S_t/\mathbf{F}_\mathfrak{p}$ is irreducible but not geometrically irreducible. For example, if $S_t/\mathbf{F}_\mathfrak{p}$ is the union of two conjugate elliptic curves defined over a quadratic extension of $\mathbf{F}_\mathfrak{p}$, then $a_\mathfrak{p}(S_t) = N_\mathfrak{p} + 1$, so (14) gives $\#S_t(\mathbf{F}_\mathfrak{p}) = 0$, as it should be.

Combine (17), (18) and (19), we get

$$\operatorname*{res}_{s=1}\sum_p \frac{-\log N_{\mathfrak{p}}}{N_{\mathfrak{p}}^{s+1}}\sum_{t\in C(\mathbf{F}_{\mathfrak{p}})} a_{\mathfrak{p}}(\mathcal{S}_t) = -\operatorname*{ord}_{s=2} L_2(S/k,s) + \operatorname*{ord}_{s=1} L(T_S,s). \tag{20}$$

T_S is a finite dimensional $\mathbf{Q}[G_k]$-module, so $L(T_S,s)$ is an Artin L-function. In particular, the second term on the right side of (20) is $-\text{rank}T_S(k)$. Under Tate's conjecture, the first term on the right side of (20) is $\text{rank}NS(S/k)$. Invoke the Shioda-Tate isomorphism (13) and we get Theorem 1.

□

4. Fiber powers of semistable elliptic fibrations

Proof of Theorem 2. Let $f:\mathcal{E}\to C$ be a semistable elliptic fibration over a number field k. Fix an integer $n\geq 2$. Then

$$\begin{aligned}
\sum_{t\in C(\mathbf{F}_{\mathfrak{p}})} a_{\mathfrak{p}}(\mathcal{E}_t)^n &= \sum_{t\in C(\mathbf{F}_{\mathfrak{p}})} (N_{\mathfrak{p}}+1-\#\mathcal{E}_t(\mathbf{F}_{\mathfrak{p}}))^n \\
&= \sum_{j=0}^{n}(-1)^j\binom{n}{j}(N_{\mathfrak{p}}+1)^{n-j}\sum_{t\in C(\mathbf{F}_{\mathfrak{p}})}\#\mathcal{E}_t(\mathbf{F}_{\mathfrak{p}})^j \\
&= \#C(\mathbf{F}_{\mathfrak{p}})(N_{\mathfrak{p}}+1)^n + \sum_{j=1}^{n}(-1)^j\binom{n}{j}(N_{\mathfrak{p}}+1)^{n-j}\cdot\#\mathcal{E}^{(j)}(\mathbf{F}_{\mathfrak{p}}), \qquad (21)
\end{aligned}$$

where $\mathcal{E}^{(j)}$ denotes the fiber product of j copies of $\mathcal{E}$ with itself over C. Denote by $\widetilde{\mathcal{E}}^{(j)}$ Deligne's desingularization of $\mathcal{E}^{(j)}$ [3] via a canonical sequence of blowups. See [19, §2] for a description of the desingularization. Write

$$b_j := \text{the number of } k\text{-rational exceptional divisors of } \widetilde{\mathcal{E}}^{(j)}.$$

Since $\mathcal{E}^{(1)}=\mathcal{E}$ is smooth, we have $b_1=0$. For $\widetilde{\mathcal{E}}^{(2)}$ the singular locus consists of isolated ordinary double points. Write $O_{\mathcal{E}}(\cdot)$ for the usual big-O notation with the constant depending on $\mathcal{E}$ only (and not on $\mathfrak{p}$); as usual the constant could change from line to line. Then

$$\#\mathcal{E}^{(j)}(\mathbf{F}_{\mathfrak{p}}) = \#\widetilde{\mathcal{E}}^{(j)}(\mathbf{F}_{\mathfrak{p}}) + b_j(N_{\mathfrak{p}}^j + O_{\mathcal{E}}(N_{\mathfrak{p}}^{j-1})).$$

Substitute this into (21) and expand $(N_{\mathfrak{p}}+1)^{n-j}$ using the binomial theorem, we get

$$\begin{aligned}
&(N_{\mathfrak{p}}+1)^n(N_{\mathfrak{p}}+1-a_{\mathfrak{p}}(C)) \\
&+\sum_{j=1}^{n}(-1)^j\binom{n}{j}\sum_{l=0}^{n-j}\binom{n-j}{l}N_{\mathfrak{p}}^l\times\Big[\#\widetilde{\mathcal{E}}^{(j)}(\mathbf{F}_{\mathfrak{p}}) - (N_{\mathfrak{p}}^j + O_{\mathcal{E}}(N_{\mathfrak{p}}^{j-1}))\cdot b_j\Big].
\end{aligned}$$

Set $tr^i_{\mathfrak{p}}(\widetilde{\mathcal{E}}^{(j)}) := \mathrm{trace}(\mathrm{Frob}_{\mathfrak{p}}, H^i(\widetilde{\mathcal{E}}^{(j)}, \mathbf{Q}_l))$. Then $\#\widetilde{\mathcal{E}}^{(j)}(\mathbf{F}_{\mathfrak{p}}) = \sum_{j=0}^{2j+2}(-1)^j tr^i_{\mathfrak{p}}(\widetilde{\mathcal{E}}^{(j)})$ by the Weil conjecture, so (21) becomes

$$\begin{aligned}
& N_{\mathfrak{p}}^{n+1} + (n+1)N_{\mathfrak{p}}^n - N_{\mathfrak{p}}^n a_{\mathfrak{p}}(C) + O_{\mathcal{E}}(N_{\mathfrak{p}}^{n-1}) \\
& + \sum_{j=1}^{n}(-1)^j \binom{n}{j} \sum_{l=0}^{n-j} \binom{n-j}{l} N_{\mathfrak{p}}^l \times \Big[\sum_{i=0}^{2j+2}(-1)^i tr^i_p(\widetilde{\mathcal{E}}^{(j)}) - b_j N_{\mathfrak{p}}^j + O_{\mathcal{E}}(N_{\mathfrak{p}}^{j-1})\Big] \\
(22) \quad = \; & N_{\mathfrak{p}}^{n+1} + (n+1)N_{\mathfrak{p}}^n - N_{\mathfrak{p}}^n a_{\mathfrak{p}}(C) + O_{\mathcal{E}}(N_{\mathfrak{p}}^{n-1}) \\
(23) \qquad & + \sum_{j=1}^{n}(-1)^j \binom{n}{j} \sum_{l=0}^{n-j} \binom{n-j}{l} N_{\mathfrak{p}}^l \times \sum_{i=0}^{2j+2}(-1)^i tr^i_p(\widetilde{\mathcal{E}}^{(j)}) \\
(24) \qquad & - N_{\mathfrak{p}}^n \sum_{j=1}^{n}(-1)^j \binom{n}{j} b_j + O_{\mathcal{E}}(N_{\mathfrak{p}}^{n-1}).
\end{aligned}$$

Lemma 1. *Suppose f has a section. Then for every $j > 0$ we have $tr^1_{\mathfrak{p}}(\widetilde{\mathcal{E}}^{(j)}) = a_{\mathfrak{p}}(C)$.*

Proof. The semistable fibration $f : \mathcal{E} \to C$ induces a fibration $\tilde{p}(j) : \widetilde{\mathcal{E}}^{(j)} \to C$. Schoen [18, Lem. 1] shows that $\tilde{p}(j)$ induces an isomorphism of fundamental groups $\pi_1(\widetilde{\mathcal{E}}^{(j)} \otimes \mathbf{C}) \to \pi_1(C \otimes \mathbf{C})$ when $j = 2$; his argument[5] applies *mutatis mutandis* for $j > 2$ as well. By the compatibility of l-adic cohomology with Betti cohomology, $\tilde{p}(j)_* : H^1_{\text{ét}}(\widetilde{\mathcal{E}}^{(j)} \otimes \overline{k}, \mathbf{Q}_l) \to H^1_{\text{ét}}(C \otimes \overline{k}, \mathbf{Q}_l)$ is then a G_k-equivariant isomorphism for $j > 1$. When $j = 1$, Raynaud's exact sequence (11) implies that $\tilde{p}(j)_*$ is also an isomorphism. The Lemma then follows.

□

Invoke the Lemma and we see that (22) + (23) is equal to

[5] which calls for f to have a section.

$$\begin{aligned}
& N_{\mathfrak{p}}^{n+1} + (n+1)N_{\mathfrak{p}}^{n} - N_{\mathfrak{p}}^{n} a_{\mathfrak{p}}(C) + O_{\mathcal{E}}(N_{\mathfrak{p}}^{n-1}) \\
& + \sum_{j=1}^{n} (-1)^{j} \binom{n}{j} \Big[N_{\mathfrak{p}}^{n-j} + (n-j)N_{\mathfrak{p}}^{n-j-1} + O_{\mathcal{E}}(N_{\mathfrak{p}}^{n-j-2}) \Big] \times \\
& \qquad\qquad \Big[N_{\mathfrak{p}}^{j+1} - N_{\mathfrak{p}}^{j} a_{\mathfrak{p}}(C) + N_{\mathfrak{p}}^{j-1} tr_{\mathfrak{p}}^{2}(\widetilde{\mathcal{E}}^{(j)}) + O_{\mathcal{E}}(N_{\mathfrak{p}}^{j-1/2}) \Big] \\
= \; & N_{\mathfrak{p}}^{n+1} + (n+1)N_{\mathfrak{p}}^{n} - N_{\mathfrak{p}}^{n} a_{\mathfrak{p}}(C) + O_{\mathcal{E}}(N_{\mathfrak{p}}^{n-1}) \\
& + \sum_{j=1}^{n} (-1)^{j} \binom{n}{j} \Big[N_{\mathfrak{p}}^{n+1} - N_{\mathfrak{p}}^{n} a_{\mathfrak{p}}(C) + (n-j)N_{\mathfrak{p}}^{n} + N_{\mathfrak{p}}^{n-1} tr_{\mathfrak{p}}^{2}(\widetilde{\mathcal{E}}^{(j)}) + O_{\mathcal{E}}(N_{\mathfrak{p}}^{n-1/2}) \Big] \\
= \; & \big(N_{\mathfrak{p}}^{n+1} - N_{\mathfrak{p}}^{n} a_{\mathfrak{p}}(C) \big) \sum_{j=0}^{n} (-1)^{j} \binom{n}{j} + N_{\mathfrak{p}}^{n} \Big[n+1 + \sum_{j=1}^{n} (-1)^{j} \binom{n}{j} (n-j) \Big] \\
& + N_{\mathfrak{p}}^{n-1} \sum_{j=1}^{n} (-1)^{j} \binom{n}{j} tr_{\mathfrak{p}}^{2}(\widetilde{\mathcal{E}}^{(j)}) + O_{\mathcal{E}}(N_{\mathfrak{p}}^{n-1/2}) \\
= \; & N_{\mathfrak{p}}^{n} + N_{\mathfrak{p}}^{n-1} \sum_{j=1}^{n} (-1)^{j} \binom{n}{j} tr_{\mathfrak{p}}^{2}(\widetilde{\mathcal{E}}^{(j)}) + O_{\mathcal{E}}(N_{\mathfrak{p}}^{n-1/2})
\end{aligned}$$

since $\sum_{j=0}^{n} (-1)^{j} \binom{n}{j} (n-j) = 0$ for $n > 1$. Thus

$$\operatorname*{res}_{s=1} \sum_{\mathfrak{p}} \frac{-\log N_{\mathfrak{p}}}{N_{\mathfrak{p}}^{s+n}} \sum_{t \in C(\mathbf{F}_{\mathfrak{p}})} a_{\mathfrak{p}}(\mathcal{E}_t)^n = \operatorname*{res}_{s=1} \sum_{\mathfrak{p}} \frac{-\log N_{\mathfrak{p}}}{N_{\mathfrak{p}}^{s}} \Big(1 - \sum_{j=1}^{n} (-1)^{j} \binom{n}{j} b_j \Big) \tag{25}$$

$$+ \sum_{j=1}^{n} (-1)^{j} \binom{n}{j} \operatorname*{res}_{s=1} \sum_{\mathfrak{p}} \frac{-\log N_{\mathfrak{p}}}{N_{\mathfrak{p}}^{s+1}} tr_{\mathfrak{p}}^{2}(\widetilde{\mathcal{E}}^{(j)}) \tag{26}$$

$$= -1 + \sum_{j=1}^{n} (-1)^{j} \binom{n}{j} \Big[\operatorname*{ord}_{s=2} L_2(\widetilde{\mathcal{E}}^{(j)}, s) + b_j \Big]. \tag{27}$$

Apply Tate's conjecture and we get Theorem 2.

□

5. Néron-Severi groups of fiber squares

Let $f : \mathcal{E} \rightarrow C$ be a semistable fibration over k. Fix a non-zero, k-rational divisor d_0 on C/k over which f is smooth. Set $F_{\mathcal{E}} := f^{-1}(d_0)$. A different choice of d_0 gives rise to another vertical fiber whose image in $NS(\mathcal{E}/k) \otimes \mathbf{Q}$ is a non-zero $\mathbf{Q}$-multiple of that of $F_{\mathcal{E}}$.

Denote by $\{t\}_{t \in \tau}$ the set of k-rational, irreducible divisors of C/k over which $f : \mathcal{E} \rightarrow C$ is singular. Since f is semistable, for every t the fiber $f^{-1}(t)$ is a sum $\sum_{i=1}^{m(t)} A_i(t)$ of pairwise distinct, k-irreducible divisors on the surface $\mathcal{E}$. Suppose further than $\mathcal{E}$ has a zero section $0_{\mathcal{E}}$. Then for each $t \in \tau$ exactly one $A_i(t)$ intersects non-trivially with $0_{\mathcal{E}}$. Relabel the components if necessary, we can assume that $A_1(t) \cap 0_{\mathcal{E}} \neq \emptyset$ for every t. The Shioda-Tate Theorem (Theorem 8) says that $NS(\mathcal{E}/k) \otimes \mathbf{Q}$ has a basis consisting of

(i) a set of generator $\{s_i\}_{i \in I}$ of the group of sections of $f : \mathcal{E} \rightarrow C$ modulo torsions,

(ii) the zero section $0_{\mathcal{E}}$,
(iii) a vertical fiber $F_{\mathcal{E}}$, and
(iv) the components $\{A_i(t)\}_{i>1}$ for each $t \in \tau$.

Since $f^{-1}(t) = \sum_{i=1}^{m(t)} A_i(t)$ is a non-zero multiple of $F_{\mathcal{E}}$ in $NS(\mathcal{E}/k) \otimes \mathbf{Q}$, for (iv) above we could leave out any one of the $A_i(t)$, not just $A_1(t)$; we choose $A_1(t)$ to facilitate future calculations.

Denote by $\pi_i : \mathcal{E}^{(2)} \to \mathcal{E}$ the two projections

$$\begin{tikzcd}
\mathcal{E}^{(2)} \arrow[r, "\pi_1"] \arrow[d, "\pi_2"'] & \mathcal{E} \arrow[d, "f"] \\
\mathcal{E} \arrow[r, "f"] & C.
\end{tikzcd}$$

Then we have a natural collection of k-rational divisors on $\mathcal{E}^{(2)}$:

$$(28) \qquad \begin{cases} S_{ij} & := \ \pi_i^{-1}(s_j), \ \text{where } i = 1,2 \text{ and } j \in I, \\ A_{ij}(t) & := \ \pi_i^{-1} A_j(t), \ \text{where } i = 1,2, \text{ and } 1 < j \leq m(t) \text{ with } t \in \tau, \\ F^{(2)} & := \ F_{\mathcal{E}} \times_C F_{\mathcal{E}}, \\ E_i & := \ \pi_i^{-1}(0_{\mathcal{E}}), \ i = 1,2, \quad \text{and} \\ \Delta & := \ \{(e,e) \in \mathcal{E}^{(2)} \subset \mathcal{E} \times \mathcal{E} : e \in \mathcal{E}\}, \end{cases}$$

where in the definition of Δ we view $\mathcal{E}^{(2)}$ as a subset of $\mathcal{E} \times \mathcal{E}$. The singular locus of $\mathcal{E}^{(2)}/\overline{k}$ consists of finitely many ordinary double points. These points break up into a finite set of k-conjugate orbits $\{l\}_{l \in L}$. Denote by $\beta : \widetilde{\mathcal{E}}^{(2)} \dashrightarrow \mathcal{E}^{(2)}$ the blowup of $\mathcal{E}^{(2)}$ at *all* of these double points, and for each $l \in L$, denote by B_l the exceptional divisor over l. Theorem 3 would follow if we can show that the following collection of divisors

$$(29) \qquad \begin{cases} \tilde{S}_{ij} := \beta^{-1}(S_{ij}), \ \tilde{A}_{ij}(t) := \beta^{-1}(A_{ij}(t)), \ \tilde{F}^{(2)} := \beta^{-1}(F^{(2)}), \\ \tilde{E}_i := \beta^{-1}(E_i), \ \tilde{\Delta} := \beta^{-1}(\Delta), \ \text{and the blowup divisors } B_l \end{cases}$$

are linearly independent[6] in $NS(\mathcal{E}^{(2)}/k) \otimes \mathbf{Q}$. Note that the number of these divisors is

$$\begin{aligned} & 2(\#I) + \sum_{t \in \tau} 2(m(t) - 1) + 4 + (\#L) \\ (30) \qquad = \ & 2 \text{ rank } NS(\mathcal{E}/k) + (\#k\text{-rational points of } \mathcal{E}^{(2)}) \end{aligned}$$

by the Shioda-Tate Theorem. Since blowing up the k-Galois orbit of an ordinary double point increases by one the rank of the Picard group over k, and hence the Néron-Severi group over k, it suffices to show that the divisors in the list (28) are linearly independent in $NS(\mathcal{E}^{(2)}/k) \otimes \mathbf{Q}$. Note that these divisors are all Cartier: $A_{ij}, S_{ij}, F^{(2)}$ and E_i are pull-back of Cartier divisors on $\mathcal{E}$, and Δ is the intersection of a Cartier divisor on $\mathcal{E} \times \mathcal{E}$ with the subvariety $\mathcal{E}^{(2)}$.

Suppose there is a relation of the form

$$R := \sum_t \sum_{i=1,2} \sum_{j>1} \alpha_{ij}(t) A_{ij}(t) + \sum_{i=1,2} \sum_{j>1} \sigma_{ij} S_{ij} + \gamma F^{(2)} + \delta \Delta + \sum_{i=1,2} \epsilon_i E_i = 0 \quad \text{in } NS(\mathcal{E}^{(2)})$$

[6] Instead of the $A_{ij}(t)$, it might seem more natural to work with $A_{j_1}(t) \times_C A_{j_2}(t)$. However, these elements turn out to be dependent in $NS(\widetilde{\mathcal{E}}^{(2)}/k) \otimes \mathbf{Q}$; cf. Remark 3 in the Introduction.

with $\alpha_{ij}(t), \sigma_{ij}, \gamma, \delta, \epsilon_i \in \mathbf{Q}$. We can find a non-zero, k-rational divisor d_1 on C which is disjoint from every $t \in \tau$ and from d_0 (recall that $F_{\mathcal{E}} := f^{-1}(d_0)$), and that $G := f^{-1}(d_1)$ intersects transversely with every S_{ij}, Δ and E_i. Then

$$G \cdot A_{ij} = G \cdot F = 0.$$

The relation $R \cdot G = 0$ then says that

$$\sum_{i=1,2} \sum_{j>1} \sigma_{ij}(S_{ij} \cdot G) + \delta(\Delta \cdot G) + \sum_{i=1,2} \epsilon_i(E_i \cdot G) = 0 \tag{31}$$

in $NS(G/k) \otimes \mathbf{Q}$. Since f is semistable, infinitely many of the fibers of f (over $\overline{k}$) are elliptic curves without complex multiplication. Thus we can assume that $G \simeq \mathcal{E}_{d_1} \times \mathcal{E}_{d_1}$, where $\mathcal{E}_{d_1} := f^{-1}(d_1)$ is the Galois orbit over k of an elliptic curve over $\overline{k}$ without complex multiplication. Consequently, $NS(\mathcal{E}_{d_1} \times \mathcal{E}_{d_1}/k) \otimes \mathbf{Q}$ is generated by three independent k-rational divisors, namely $\mathcal{E}_{d_1} \times 0, 0 \times \mathcal{E}_{d_1}$ and the diagonal divisor on $\mathcal{E}_{d_1} \times \mathcal{E}_{d_1}$; and we have the identification

$$\begin{aligned} &S_{1j} \cdot G \sim 0 \times \mathcal{E}_{d_1}, \quad E_1 \cdot G \sim \mathcal{E}_{d_1} \times 0, \quad \Delta \cdot G \sim \text{ diagonal divisor on } \mathcal{E}_{d_1} \times \mathcal{E}_{d_1}, \\ &S_{2j} \cdot G \sim \mathcal{E}_{d_1} \times 0, \quad E_2 \cdot G \sim 0 \times \mathcal{E}_{d_1}. \end{aligned}$$

Then (31) implies that (among other things)

$$\delta = 0. \tag{32}$$

Next, consider the intersection of R with $E_1 \simeq \mathcal{E}/k$. Note that

$$S_{1j} \cdot E_1 = 0 \quad \text{for all } j,$$

and we have the identification

$$A_{2j}(t) \cdot E_1 \sim A_j(t), \quad S_{2j} \cdot E_1 \sim s_j, \quad F^{(2)} \cdot E_1 \sim F_{\mathcal{E}}, \quad E_2 \cdot E_1 \sim 0_{\mathcal{E}}$$

in $NS(E_1/k) \otimes \mathbf{Q} \simeq NS(\mathcal{E}/k) \otimes \mathbf{Q}$. Recall that $A_j(t)$ intersects trivially with $0_{\mathcal{E}}$ for all $j > 1$, so

$$A_{1j}(t) \cdot E_1 = 0 \quad \text{for all } j > 1.$$

We claim that $E_1 \cdot E_1 = 0$; in light of the identifications above the relation $R \cdot E_1 = 0$ then becomes

$$\sum_{t} \sum_{j>1} \alpha_{2j}(t) A_j(t) + \sum_{j>1} \sigma_{2j} s_j + \gamma F_{\mathcal{E}} + \epsilon_2 0_{\mathcal{E}} = 0$$

in $NS(E_1/k) \otimes \mathbf{Q} \simeq NS(\mathcal{E}/k) \otimes \mathbf{Q}$. The Shioda-Tate Theorem then implies that

$$\sigma_{2j} = \alpha_{2j} = \gamma = \epsilon_2 = 0.$$

for every j. Repeat the same argument for $R \cdot E_2$ and we get that $\sigma_{1j} = \alpha_{1j} = \epsilon_1 = 0$ for every j. All in all, these calculations show that the divisors in (29) are independent modulo numerical equivalence, and hence they are independent modulo algebraic equivalence tensored with $\mathbf{Q}$.

It remains to show that $E_1 \cdot E_1 = 0$ in $NS(\mathcal{E}^{(2)}/k) \otimes \mathbf{Q}$. For that we need an auxilary result.

Lemma 2. *Let $\mathcal{E} \rightarrow C$ be an elliptic fibration over k with a zero section $0_{\mathcal{E}}$. Then there exists a divisor M on $\mathcal{E}$ which is disjoint from $0_{\mathcal{E}}$, such that $M - n0_{\mathcal{E}}$ is the divisor of a function on $\mathcal{E}$ for some integer $n > 1$.*

Proof. We can assume that $\mathcal{E}\to C$ is relatively minimal. Write $\mathcal{E}'$ for the generic fiber. Fix an integer $m > 1$. Then

$$M' \ := \ \text{kernal of the multiplication-by-}m \text{ map on } \mathcal{E}',$$

and hence $M'' := M' - \{0_{\mathcal{E}'}\}$, are both divisors on the elliptic curve $\mathcal{E}'$ over the function field K_C of C/k. Add up the points in M'' and we see that $M'' - (m^2 - 1)0_{\mathcal{E}'}$ is the divisor of a function on $\mathcal{E}'/k_C$. Since $\mathcal{E}\to C$ is relatively minimal, by the Néron property M'' extends to a divisor M on $\mathcal{E}$ which is disjoint from $0_{\mathcal{E}}$, and the Lemma follows by taking $n = m^2 - 1$.

□

Returning to the proof of $E_1 \cdot E_1 = 0$, let M and n be as in the Lemma. Then E_1 and $\mathcal{E}\times_C M$ defines the same elements in $NS(\mathcal{E}^{(2)}/k)\otimes\mathbf{Q}$, whence $E_1\cdot E_1$ is a non-zero $\mathbf{Q}$-multiple of $(\mathcal{E}\times_C 0_{\mathcal{E}})\cdot(\mathcal{E}\times_C M)$, which is zero. This completes the proof that the divisors in (28) are linearly independent in $NS(\mathcal{E}^{(2)}/k)\otimes\mathbf{Q}$, and Theorem 3 follows.

□

6. Cyclic subgroups of elliptic curves

The classical modular curve $X_0(M)$ has an open subset $Y_0(M) \subset X_0(M)$, both defined over $\mathbf{Q}$, such that for any field K of characteristic prime to N, the K-rational points of $Y_0(M)$ parameterizes equivalent classes of pairs (E, C), where E is a elliptic curve over K, and C is a K-rational cyclic subgroup of E of order M; two such pairs (E, C) and (E', C') are declared to be equivalent if there exists a K-rational isomorphism taking E to E' and C to C'. See [15] for more details.

There is a canonical map $X_0(M)\to X_0(1)$ defined over $\mathbf{Q}$ which sends a pair $(E, C) \in Y_0(M)$ to $j(E) :=$ the j-invariant of E. In preparation for the next Section we need to understand the number of $\mathbf{F}_p$-rational points on each fiber of this map. Ogg's argument in [15, Thm. 2] applies *mutatis mutandis* and yields the following result.

Lemma 3. *Fix $j \in \mathbf{F}_p$ with $j \neq 0, 1728$. Choose any elliptic curve $E/\mathbf{F}_p$ with $j(E) = j$. Then the number of equivalent classes of pairs (E', C') in $Y_0(M)(\mathbf{F}_p)$ with $j(E') = j$ and $a_p(E) = a_p(E')$, is equal to* <u>*one half*</u> *of*

$$N_{E,p}(M) := \textit{the number of } \mathbf{F}_p\textit{-rational cyclic subgroups of } E \textit{ of order } M.$$

□

Set $d_{E,p} := a_p(E)^2 - 4p$. When M is prime to $2d_E$, Ogg [15, Prop. 2] shows that

$$N_{E,p}(M) = \prod_{q|d} \left(1 + \left(\frac{d_{E,p}}{q}\right)\right), \tag{33}$$

where q runs through all distinct prime divisors of M. Utilizing techniques from Waterhouse's thesis [29], Ito [7] evaluates $N_{E,p}(M)$ in all cases. For the rest of this section, we state Ito's Theorem and rewrite his expression for $N_{E,p}(M)$ in a form suitable for our subsequent application. Clearly it suffices to work with the case where M is a prime power. We begin by setting up some notation.

Let $E/\mathbf{F}_p$ be an ordinary elliptic curve, so $a := a_p(E)$ lies between $\pm 2\sqrt{p}$ and $a \neq 0$. Denotes by $\pi_a, \overline{\pi}_a$ the two distinct roots of $h_{a,p}(x) := x^2 - ax + p$. Fix a prime l. Set

$$\begin{aligned} c_a &:= \text{the conductor of the order } \mathbf{Z}[\pi_a], \\ \epsilon_a &:= \operatorname{ord}_l(c_a). \end{aligned}$$

Then $\operatorname{End}_{\mathbf{F}_p}(E)$ is an order in the imaginary quadratic field $\mathbf{Q}(\pi_a)$ containing $\mathbf{Z}[\pi_a]$. The converse also holds.

Lemma 4 (Waterhouse [29, Thm. 4.2])**.** *If $a \neq 0$, then any order in $\mathbf{Q}(\pi_a)$ containing $\mathbf{Z}[\pi_a]$ is the endomorphism ring of some elliptic curve over $\mathbf{F}_p$ with $p+1-a$ points over $\mathbf{F}_p$.*

□

Theorem 9 (Ito [7])**.** *Let $E/\mathbf{F}_p$ be ordinary. With the notation as above, set*

$$\begin{aligned} c_E &:= \textit{the conductor of } End_{\mathbf{F}_p}(E), \\ \epsilon_E &:= ord_l(c_E). \end{aligned}$$

Then $\epsilon_E \leq \epsilon_a$, and

(i) *if $1 \leq \epsilon \leq \epsilon_a - \epsilon_E$ then $N_{E,p}(l^\epsilon) = (l+1)l^{\epsilon-1}$;*
(ii) *if $\epsilon_a - \epsilon_E < \epsilon \leq \epsilon_a + \epsilon_E$, then $N_{E,p}(l^\epsilon) = l^{[(\epsilon+\epsilon_a-\epsilon_E)/2]}$;*
(iii) *If $\epsilon > \epsilon_a + \epsilon_E$, then*

$$N_{E,p}(l^\epsilon) = \begin{cases} 2l^{\epsilon_a} & \textit{if } l \textit{ splits in } \mathbf{Q}(\pi_a), \\ 0 & \textit{if } l \textit{ is inert in } \mathbf{Q}(\pi_a), \\ l^{\epsilon_a} & \textit{if } l \textit{ ramifies and } \epsilon = \epsilon_a + \epsilon_E + 1, \\ 0 & \textit{if } l \textit{ ramifies and } \epsilon > \epsilon_a + \epsilon_E + 1. \end{cases}$$

□

Corollary 3. *If $E/\mathbf{F}_p$ is ordinary, then $N_{E,p}(l^\epsilon)$ depends only on ϵ_a and ϵ_E.*

□

Remark 11. Ito also determines $N_{E,p}(l^\epsilon)$ when $E/\mathbf{F}_p$ is supersingular; again the answer depends only on ϵ_a and ϵ_E. We do not reproduce the result here since the supersingular case will not arise in our application. Also, note that Ogg's formula (33) is in agreement with (case (iii) of) Ito's Theorem.

The Corollary suggests a new notation. Given a and p as above, let $f > 0$ be an integer with $f^2 | (a^2 - 4p)$ and $(a^2-4p)/f^2 \equiv 0, 1 \pmod 4$. Then $\mathbf{Q}(\pi_a)$ has a unique order of discriminant $(a^2-4p)/f^2$ which contains $\mathbf{Z}[\pi_a]$, and which, by Lemma 4, corresponds to the endomorphism ring of some elliptic curve $E/\mathbf{F}_p$ with $p+1-a$ points. If E, E' are two such curves, Ito's Theorem says that $N_{E,p}(M) = N_{E',p}(M)$ for all M. Thus

$$N_{a,f,p}(l^\epsilon) := N_{E,p}(l^\epsilon)$$

is well-defined. We now come to the main result of this section.

Lemma 5. *Let $M > 0$ be odd. Set $M_f := (M, f)$. Then we have the equality*

$$N_{a,f,p}(M) = \frac{\Psi(M)}{\Psi(M/M_f)} \sigma(a, f, p, M),$$

where $\Psi(m) := m\prod_{q|m}(1+1/q)$, *$q$ runs through the prime divisors of m; and*

$$\sigma(a,f,p,M) = \#\{x \,(\mathrm{mod}\, M) : x^2 - ax + p \equiv 0 \,(\mathrm{mod}\, M_f M)\}.$$

Remark 12. Note that the x's in $\sigma(a,f,p,M)$ are well-defined: since M_f divides the conductor of $\mathbf{Z}[\pi_a]$, if $h_{a,p}(\pi) \equiv 0 \,(\mathrm{mod}\, M_f M)$ then π is a double root of $h \,(\mathrm{mod}\, M_f M)$, whence $h'_{a,p}(\pi) \equiv 0 \,(\mathrm{mod}\, M)$. Thus for any $\lambda \equiv 0 \,(\mathrm{mod}\, M)$ we have $h_{a,p}(\pi+\lambda) = h_{a,p}(\pi) + h'_{a,p}(\pi)\lambda + \lambda^2 \equiv 0 \,(\mathrm{mod}\, M_f M)$, as desired.

Proof. It suffices to assume that M is an odd-prime power l^ϵ, and ϵ_E in Ito's Theorem is equal to

$$\epsilon_f := \mathrm{ord}_l(c_a/f).$$

The two cases $1 \le \epsilon_a - \epsilon_f$ and $\epsilon_a - \epsilon_f < \epsilon \le \epsilon_a + \epsilon_f$ are immediate consequence of the first part of the following Lemma.

Lemma 6. *Let $g \in \mathbf{Z}[x]$ be monic and quadratic, and let $l > 2$ be a prime.*

(a) *Suppose $l^{2m_0}|disc(g)$. Then for any integer $1 \le m \le m_0$,*

$$\#\{x \,(\mathrm{mod}\, l^m) : g(x) \equiv 0 \,(\mathrm{mod}\, l^m)\} = l^{m_0 - [(m+1)/2]}.$$

Moreover, there exists a unique $x \,(\mathrm{mod}\, l^{m_0})$ such that $g(x) \equiv 0 \,(\mathrm{mod}\, l^{2m_0})$.

(b) *If $l||disc(g)$, then $g(x)$ has a unique solution $(\mathrm{mod}\, l)$ and has no solution $(\mathrm{mod}\, l^n)$ for any $n > 1$.*

Proof. Write $g(x) = x^2 - ax + b$. Since $l > 2$,

$$g(a/2) = -(a^2 - 4b)/4 \equiv 0 \,(\mathrm{mod}\, l^{2m_0})$$

by hypothesis. Furthermore, the quadratic formula shows that $a/2$ is a double root of $g \,(\mathrm{mod}\, l^{m_0})$, whence $g'(a/2) \equiv 0 \,(\mathrm{mod}\, l^{m_0})$. Thus for any $\beta \in \mathbf{Z}$ and any $m \le m_0$,

$$g(a/2+\beta) = g(a/2) + g'(a/2)\beta + \beta^2 \equiv \beta^2 \,(\mathrm{mod}\, l^m) \tag{34}$$

Thus $g(a/2+\beta) \equiv 0 \,(\mathrm{mod}\, l^m)$ if and only if $\beta \equiv 0 \,(\mathrm{mod}\, l^{[(m+1)/2]})$. This gives the first part of (a). To get the second part, note that if $\beta \equiv 0 \,(\mathrm{mod}\, l^{[(m_0+1)/2]})$, then combining $l^{2m_0}|g(a/2)$ and $l^{m_0}|g'(a/2)$ with (34), we get $g(a/2+\beta) \equiv 0 \,(\mathrm{mod}\, l^{m_0+[(m_0+1)/2]})$ if and only if $\beta \equiv 0 \,(\mathrm{mod}\, l^{[(3m_0+1)/4]})$. Repeat this argument finitely many times and we get $g(a/2+\beta) \equiv 0 \,(\mathrm{mod}\, l^{2m_0})$ if and only if $\beta \equiv 0 \,(\mathrm{mod}\, l^{m_0})$, as desired.

As for Part (b), $l|\mathrm{disc}(g)$ implies that $a/2$ is also a repeated root $0 \,(\mathrm{mod}\, l)$, whence $l|g'(a/2)$ as well, and (34) shows that $g(x) \equiv 0 \,(\mathrm{mod}\, l^2)$ has at most one solution. But $g(a/2) = -(a^2-4b)/4$ is exactly divisible by l, by hypothesis.

□

Returning to the proof of the last case $\epsilon > \epsilon_a + \epsilon_f$ of Lemma 5, denote by $\mathbf{Z}[\pi_0]$ the maximal order in $\mathbf{Q}(\pi_a)$, and by $g_0 \in \mathbf{Z}[x]$ the minimal polynomial of π_0. Then $\pi_a = b + \lambda\pi_0$ for some integers b, λ with $l^{\epsilon_a}||\lambda$, so with the change of variable $z = (x-b)/\lambda$,

$$g(x) \equiv 0 \,(\mathrm{mod}\, l^{\epsilon+\epsilon_a-\epsilon_f}) \Longleftrightarrow g_0(z) \equiv 0 \,(\mathrm{mod}\, l^{\epsilon+\epsilon_a-\epsilon_f-2\epsilon_a}).$$

Thus

$$\begin{aligned} &\#\{x \,(\mathrm{mod}\, l^\epsilon) : \quad g(x) \equiv 0 \,(\mathrm{mod}\, l^{\epsilon+\epsilon_a-\epsilon_f})\} \\ = \;&\#\{z \,(\mathrm{mod}\, l^{\epsilon-\epsilon_a}) : g_0(z) \equiv 0 \,(\mathrm{mod}\, l^{\epsilon+\epsilon_a-\epsilon_f-2\epsilon_a})\}. \end{aligned}$$

If $l \nmid \mathrm{disc}(g_0)$, then the lifting argument in the proof of Hensel's Lemma shows that the number of solutions $\pmod{l^{\epsilon-\epsilon_a}}$ of $g_0(z) \equiv 0 \pmod{l^{\epsilon+\epsilon_a-\epsilon_f-2\epsilon_a}}$ is either 2 or 0, depending on whether l is split or inert in $\mathbf{Q}(\pi_a)$. This gives Lemma 5 when $\epsilon > \epsilon_a - \epsilon_f$ and $l \nmid \mathrm{disc}(g_0)$. The last subcase $l | \mathrm{disc}(g_0)$ is handled by Lemma 6(b). This completes the proof of Lemma 5.

□

We close this section with a computation we need for the next Section. Fix $\pi, \overline{\pi} \in \mathbf{C}$ so that $\pi\overline{\pi} = p \in \mathbf{Z}$. For any integer $k \geq 0$, define

$$Q(\pi, k) := \frac{\pi^{2k+1} - \overline{\pi}^{2k+1}}{\pi - \overline{\pi}}.$$

Then $Q(\pi, k) = (\pi^{2k} + \overline{\pi}^{2k}) + \mathbf{Z}$-linear combinations of $(\pi^{2i} + \overline{\pi}^{2i})$ for $0 \leq i < k$, whence $(\pi + \overline{\pi})^{2n}$ is a $\mathbf{Z}$-linear combinations of the $Q(\pi, k)$. Our goal is to determine these coefficients.

For any $n \geq 1$, write $(\pi + \overline{\pi})^{2n} = \sum_{i=0}^{n} c_p(n, i) Q(\pi, i)$. Using the identities $(\pi + \overline{\pi})^2 = Q(\pi, 1) + p$ and, for any $k > 0$, $(\pi + \overline{\pi})^2 Q(\pi, k) = Q(\pi, k+1) + 2pQ(\pi, k) + p^2 Q(\pi, k-1)$, we readily obtain the recurrence relations

$$\begin{aligned}
c_p(n+1, n+1) &= 1, \\
c_p(n+1, n) &= c_p(n, n-1) + 2p, \\
c_p(n+1, i) &= p^2 c_p(n, i+1) + 2pc_p(n, i) + c_p(n, i-1) \quad \text{for } 1 \leq i < n, \\
c_p(n+1, 0) &= p^2 c_p(n, 1) + pc_p(n, 0).
\end{aligned}$$

A simple induction then yields the desired formula: for $i < n$,

$$c_p(n, i) = (2i+1) \frac{(2n)!}{(n-i)!(n+i+1)!} p^{n-i}. \tag{35}$$

Note that every $c_p(n, i)$ is positive.

7. Elliptic modular surfaces

Proof of Theorem 4. Denote by $f_M : \mathcal{E} \rightarrow X_0(M)$ the elliptic modular surface associated to $X_0(M)$. Both f_M and $\mathcal{E}$ are defined over $\mathbf{Q}$. Shioda [22] shows that f_M is a semistable fibration, and that its group of section is finite even after we extend the base field to $\mathbf{C}$. To simplify the notation, write Y and X for $Y_0(M)$ and $X_0(M)$, respectively. Then

$$\begin{aligned}
\sum_{t \in X(\mathbf{F}_p)} a_p(\mathcal{E}_t)^n &= \sum_{a^2 < 4p} a^n \sum_{\substack{t \in X(\mathbf{F}_p) \\ a_p(\mathcal{E}_t) = a}} 1 \\
&= \sum_{a^2 < 4p} a^n \sum_{\substack{t \in Y(\mathbf{F}_p) \\ a_p(\mathcal{E}_t) = a}} 1 + O_X(1)
\end{aligned}$$

since $|a_p(\mathcal{E}_t)| \leq 1$ for every bad fiber $\mathcal{E}_t$. The number of $t \in Y(\mathbf{F}_p)$ with $j(\mathcal{E}_t) = 0$ or 1728 is at most $\deg(X_0(M) \rightarrow X_0(1)) \ll M$, so

$$\sum_{t \in X(\mathbf{F}_p)} a_p(\mathcal{E}_t)^n = \sum_{a^2 < 4p} a^n \sum_{\substack{j \in \mathbf{F}_p \\ j \neq 0, 1728}} \sum_{\substack{t \in Y(\mathbf{F}_p) \\ a_p(\mathcal{E}_t) = a \\ j(\mathcal{E}_t) = j}} 1 + O_X(p^{n/2}). \tag{36}$$

The supersingular fibers do not contribute to the sum, so for the rest of this section, we will assume that

$$j(\mathcal{E}_t) \neq 0, 1728 \text{ and } a_p(\mathcal{E}_t) \neq 0. \tag{37}$$

Thanks to Lemma 3, the inner-most sum in (36) is simply

$$\frac{1}{2} N_{E_j,p}(M) = \frac{1}{2} N_{a,f,p}(M),$$

where $E_j/\mathbf{F}_p$ is any curve with $j(E_j) = j$, and $f = c_a/c_{E_j}$ as before. As we run through all $j \in \mathbf{F}_p$ with $j \neq 0, 1728$ and $a_p(E_j) = a$, by Lemma 4 we run through precisely all integers $f > 0$ such that

$$f^2 \text{ divides } a^2 - 4p \text{ and } (a^2 - 4p)/f^2 \equiv 0, 1 \pmod 4). \tag{38}$$

The number of $E/\mathbf{F}_p$ with $E(\mathbf{F}_p) = p + 1 - a$ and with $\mathrm{End}_{\mathbf{F}_p}(E)$ equals to the order in $\mathbf{Q}(\pi_a)$ with discriminant $(a^2 - 4p)/f^2$, is equal[7] to $h((a^2 - 4p)/f^2)$, where

$$h(\Delta) \quad := \quad \text{the class number of the imaginary quadratic order of discriminant } \Delta.$$

Combine all these together, invoke Lemma 5 and we can rewrite (36) as

$$\begin{aligned} & \frac{1}{2} \sum_{a^2<4p} a^n \sum_f h\Big(\frac{a^2-4p}{f^2}\Big) N_{a,f,p}(M) + O_X(p^{n/2}) \\ = \quad & \frac{1}{2} \sum_{a^2<4p} a^n \sum_f h\Big(\frac{a^2-4p}{f^2}\Big) \frac{\Psi(M)}{\Psi(M/M_f)} \sigma(a,f,p,M) + O_X(p^{n/2}), \end{aligned} \tag{39}$$

where f runs through all integers as in (38) and $M_f = (M, f)$ as in the last Section. Since $\sigma(a, f, p, M) = \sigma(-a, f, p, M)$, if n is odd then the double sum in (39) is zero, whence the entire expression (39) is $O_X(p^{n/2})$. Substitute this back into (36) and we get, for odd n,

$$\sum_p \frac{-\log p}{p^{s+[n/2]+1}} \sum_{t \in X(\mathbf{F}_p)} a_p(\mathcal{E}_t)^n \ \ll \ \sum_p \frac{-\log p}{p^{s+[n/2]+1}} p^{n/2}.$$

Theorem 4(a) then follows. To handle even n, we rewrite (39) in terms of the Selberg trace formula for Hecke operators on cusp forms for $\Gamma_0(M)$; Theorem 4 then follows from the Weil conjecture estimate for these traces.

For any fixed p, the number of pairs (a, f) with $a^2 - 4p = -3f^2$ or $-4f^2$ is at most four. Since $N_{a,f,p}(M)$ is bounded from the above in terms of M, with

$$h_w(\Delta) := \begin{cases} h(\Delta) & \text{if } \Delta < -4 \\ 1/2 & \text{if } \Delta = -4 \\ 1/3 & \text{if } \Delta = -3 \end{cases}$$

[7] this is due to Waterhouse [29, Thm. 4.5]. However, note the correction in [20, p. 194], which does not affect us.

and recall that $a = \pi_a + \overline{\pi}_a$, for even n we can further rewrite (39) as

$$\begin{aligned} &\frac{1}{2}\sum_{a^2<4p}(\pi_a+\overline{\pi}_a)^n\sum_f h_w\Big(\frac{a^2-4p}{f^2}\Big)\frac{\Psi(M)}{\Psi(M/M_f)}\sigma(a,f,p,M)+O_X(p^{n/2}) \\ (40) = \; &\sum_{i=0}^{n/2}c_p(n/2,i)\frac{1}{2}\sum_{a^2<4p}Q(\pi_a,i)\sum_f h_w\Big(\frac{a^2-4p}{f^2}\Big)\frac{\Psi(M)}{\Psi(M/M_f)}\sigma(a,f,p,M)+O_X(p^{n/2}),\end{aligned}$$

where the $c_p(n/2,i)$ and $Q(\pi_a,i)$ are as in the end of the last Section. The Selberg trace formula says that the trace of the Hecke operator T_p on the space of weight $2k$ modular forms on $\Gamma_0(M)$ with $p \nmid M$, is given by [21, Thm. 2.2]

$$\begin{aligned}\operatorname{trace}(T_p, S_{2k}(\Gamma_0(M))) \;=\; &\frac{-1}{2}\sum_{a^2<4p}Q(\pi_a,k-1)\sum_f h_w\Big(\frac{a^2-4p}{f^2}\Big)\frac{\Psi(M)}{\Psi(M/M_f)}\sigma(a,f,p,M) \\ &-\sum_{\substack{c\mid M \\ (c,M/c)\mid(M,p-1)}}\phi((c,M/c))+\begin{cases} p+1 & \text{if } 2k=2 \\ 0 & \text{otherwise.}\end{cases}\end{aligned}$$

This allows us to rewrite (40) as

$$\begin{aligned} &c_p(n/2,0)p-\sum_{i=1}^{n/2}c_p(n/2,i)\Big[\operatorname{trace}(T_p,S_{2i}(\Gamma_0(M)))+O_X(1)\Big]+O_X(p^{n/2}) \\ = \;&\frac{p^{n/2+1}n!}{(n/2)!(n/2+1)!}+O_X(p^{n/2}),\end{aligned}$$

since the Weil conjecture gives $\operatorname{trace}(T_p, S_{2i}(\Gamma_0(M))) \ll p^{i-1/2}$ while (35) gives $c_p(k,i) \ll p^{k-i}$. Substitute these back into (36) and we get Theorem 4 for even n.

□

Remark 13. Our use of the trace formula above is inspired by the work of Birch [1] on the asymptotic behavior of *even* moments of values of $a_p(E)$ over all elliptic curves over $\mathbf{F}_p$. This is essentially the $M = 1$ case above; of course, when $M = 1$ the problem of counting cyclic M-isogenies does not arise.

8. Tate conjecture for $\mathcal{E}$ and $\widetilde{\mathcal{E}}^{(2)}$

To simplify our notation, write $\mathcal{E}$ for $\mathcal{E}_M$ and write C for $X_0(M)$. For the rest of this section the ground field is $\mathbf{Q}$.

We begin with $\mathcal{E}$. Following the notation in the Introduction, denote by $T_{\mathcal{E}}$ the subgroup of $NS(\mathcal{E}/\overline{\mathbf{Q}})$ generated by the zero section of $f : \mathcal{E} \to C$ together with all the $\overline{\mathbf{Q}}$-components of the fibers of f. From the theory of modular curves we know that these irreducible components are all defined over (subfields of) the cyclotomic field $\mathbf{Q}(\zeta_M)$. Consequently, the Artin L-function $L(T_{\mathcal{E}} \otimes \mathbf{Q}, s)$ attached to the $\mathbf{Q}[G_{\mathbf{Q}}]$-module $T_{\mathcal{E}} \otimes \mathbf{Q}$ is a product of Dirichlet L-series. In particular, $L(T_{\mathcal{E}} \otimes \mathbf{Q}, s)$ has a meromorphic continuation to $\mathbf{C}$ and is holomorphic for $Re(s) > 0$ except for a pole at $s = 1$ of order rank $T_{\mathcal{E}}(\mathbf{Q})$. On the other hand, Rosen and

Silverman [16, p. 52-53] shows that, for $\mathrm{Re}(s) > 3/4$,

$$\sum_p \frac{-\log p}{p^{s+1}} \sum_{t\in X_0(M)(\mathbf{F}_p)} a_p(\mathcal{E}_t) = -\frac{d}{ds}\log L_2(\mathcal{E}/\mathbf{Q}, s+1) + \frac{d}{ds}\log L(T_{\mathcal{E}}/\mathbf{Q}, s) + O(1).$$

By Theorem 4, the left side has an analytic continuation to $\mathrm{Re}(s) > 1$. It follows that $L_2(\mathcal{E}/\mathbf{Q}, s)$ has an analytic continuation to $Re(s) > 7/4$ except for a pole at $s = 2$ of order equal to rank $T_{\mathcal{E}}(\mathbf{Q})$. Finally, Shioda [22] shows that the group of sections of $\mathcal{E}\to C$ is finite (even when the base field is $\mathbf{C}$), so by the Shioda-Tate theorem, the order of pole of $L_2(\mathcal{E}/\mathbf{Q}, s)$ at $s = 2$ is in fact rank $NS(\mathcal{E}/\mathbf{Q})$. This completes the proof of the Tate conjecture for $\mathcal{E}/\mathbf{Q}$.

Lemma 7. $-\operatorname*{ord}_{s=2} L_2(\widetilde{\mathcal{E}}^{(2)}/\mathbf{Q}, s) \geq \mathrm{rank}\big[H^2_{\acute{e}t}(\widetilde{\mathcal{E}}^{(2)} \otimes \overline{\mathbf{Q}}, \mathbf{Q}_l(1))^{G_{\mathbf{Q}}}\big]$.

Proof. Part of the following calculation is inspired by [18, Lem. 1.6].

From the spectral sequence for $\tilde{\pi} : \widetilde{\mathcal{E}}^{(2)}\to X_0(M)$ we get a $G_{\mathbf{Q}}$-equivariant filtration on $H^2_{\text{ét}}(\widetilde{\mathcal{E}}^{(2)} \otimes \overline{\mathbf{Q}}, \mathbf{Q}_l) =: L^0$ with

$$L^2 \simeq H^2(R^0), \quad L^1/L^2 \simeq H^1(R^1), \quad L^0/L^1 \simeq H^0(R^2),$$

where $H^i(R^j) := H^i_{\text{ét}}(X_0(M) \otimes \overline{\mathbf{Q}}, R^j\tilde{\pi}_*\mathbf{Q}_{l,\widetilde{\mathcal{E}}^{(2)}})$. Thus $L_2(\widetilde{\mathcal{E}}^{(2)}/\mathbf{Q}, s)$ is the product of the L-functions associated to $H^{2-t}(R^t)$ for $t = 0, 1, 2$. Moreover,

$$\sum_{t=0}^{2} \mathrm{rank}\big[H^{2-t}(R^t)(1)^{G_{\mathbf{Q}}}\big] \geq \mathrm{rank}\big[H^2_{\text{ét}}(\widetilde{\mathcal{E}}^{(2)} \otimes \overline{\mathbf{Q}}, \mathbf{Q}_l(1))^{G_{\mathbf{Q}}}\big]. \tag{41}$$

To prove the Lemma it then suffices to show that for every t,

$$-\operatorname*{ord}_{s=2} L(H^{2-t}(R^t), s) \geq \mathrm{rank}\big[H^{2-t}(R^t)(1)^{G_{\mathbf{Q}}}\big]. \tag{42}$$

We begin with $t = 0$. Since $R^0\tilde{\pi}_*\mathbf{Q}_{l,\widetilde{\mathcal{E}}^{(2)}} \simeq \mathbf{Q}_{l,X_0(M)}$, we have $H^2(R^0) \simeq \mathbf{Q}_l(-1)$. In particular, $\mathrm{trace}(\mathrm{Frob}_p, H^2(R^0)) = p$. Thus $L(H^2(R^0), s) = \zeta(s-1)$ has a simple pole at $s = 2$ while $\mathrm{rank} H^2(R^0)(1)^{G_{\mathbf{Q}}} = 1$, so both sides of (42) are 1 when $t = 0$.

Denote by Z the singular locus of $f : \mathcal{E}\to C$; it is also the singular locus for $\widetilde{\mathcal{E}}^{(2)}\to C$. Denote by $i : Z\to C$ the closed immersion, and by $j : U\to C$ the open embedding of $U = C - Z$ in C. For any l-adic sheaf $\mathcal{F}$ on C we have an exact sequence

$$0\to i_*i^!\mathcal{F}\to\mathcal{F}\to j_*j^*\mathcal{F}.$$

This becomes a short exact sequence for $\mathcal{F} = R^t\tilde{\pi}_*\mathbf{Q}_{l,\widetilde{\mathcal{E}}^{(2)}}$, by the local invariant cycle theorem. Moreover,

$$\begin{aligned} j^*R^t\tilde{\pi}_*\mathbf{Q}_{l,\widetilde{\mathcal{E}}^{(2)}} &\simeq R^t\pi_{U*}(j^*_{\mathcal{E}})\mathbf{Q}_{l,\widetilde{\mathcal{E}}^{(2)}} \qquad \text{proper base change} \\ &\simeq R^t\pi_{U*}\mathbf{Q}_{l,\mathcal{E}^{(2)}_U}, \end{aligned}$$

where $f_U : \mathcal{E}_U\to U$ is the pull-back to U of $f : \mathcal{E}\to C$ via j and $\pi_U : \mathcal{E}^{(2)}_U\to U$ the corresponding map. Consequently,

$$\mathrm{trace}(\mathrm{Frob}_p, H^{2-t}(R^t)) = \mathrm{trace}(\mathrm{Frob}_p, H^{2-t}_{\text{ét}}(X_0(M) \otimes \overline{\mathbf{Q}}, i_*i^!R^t\tilde{\pi}_*\mathbf{Q}_{l,\widetilde{\mathcal{E}}^{(2)}})) + \tag{43}$$

$$\mathrm{trace}(\mathrm{Frob}_p, H^{2-t}_{\text{ét}}(X_0(M) \otimes \overline{\mathbf{Q}}, j_*R^t\pi_{U*}\mathbf{Q}_{l,\mathcal{E}^{(2)}_U})). \tag{44}$$

Since $i_* i^! \mathcal{F}$ is a skyscraper sheaf, for $t = 1$ the Kunneth formula gives

$$\begin{aligned} \mathrm{trace}(\mathrm{Frob}_p, H^1(R^1)) &= \mathrm{trace}(\mathrm{Frob}_p, H^1_{\text{ét}}(X_0(M) \otimes \overline{\mathbf{Q}}, j_* R^1 \pi_{U*} \mathbf{Q}_{l,\mathcal{E}_U^{(2)}})) \\ & \mathrm{trace}(\mathrm{Frob}_p, H^1_{\text{ét}}(X_0(M) \otimes \overline{\mathbf{Q}}, j_* R^1 f_{U*} \mathbf{Q}_{l,\mathcal{E}_U}))^{\oplus 2}. \end{aligned}$$

Deligne [3] shows that $H^1_{\text{ét}}(X_0(M) \otimes \overline{\mathbf{Q}}, j_* R^1 f_{U*} \mathbf{Q}_{l,\mathcal{E}_U})$ is canonically identified with the space of weight 3 modular forms on $\Gamma_0(M)$ plus its complex conjugate. There are no weight 3 modular forms on $\Gamma_0(N)$, so for $t = 1$ both sides of (42) are zero.

Finally, consider the case $t = 2$. The Kunneth formula gives

$$\begin{aligned} & H^0_{\text{ét}}(X_0(M) \otimes \overline{\mathbf{Q}}, j_* R^2 \tilde{\pi}_{U*} \mathbf{Q}_{l,\mathcal{E}_U^{(2)}}) \\ \simeq \; & H^0_{\text{ét}}(X_0(M) \otimes \overline{\mathbf{Q}}, j_* \underbrace{R^2 \tilde{f}_{U*} \mathbf{Q}_{l,\mathcal{E}_U}}_{\mathbf{Q}_l(-1)})^{\oplus 2} \oplus H^0_{\text{ét}}(X_0(M) \otimes \overline{\mathbf{Q}}, j_* \underbrace{(R^1 \tilde{f}_{U*} \mathbf{Q}_{l,\mathcal{E}_U})^{\otimes 2}}_{\mathbf{Q}_l(-1)}). \\ \simeq \; & \mathbf{Q}_l(-1)^{\oplus 2} \oplus \mathbf{Q}_l(-1), \end{aligned}$$

so (44) contributes 3 to both sides of (42). As for (43),

$$H^0_{\text{ét}}(X_0(M) \otimes \overline{\mathbf{Q}}, i_* i^! R^2 \tilde{\pi}_* \mathbf{Q}_{l,\widetilde{\mathcal{E}}^{(2)}}) \simeq \oplus_x H^0_{\text{ét}}(x \otimes \overline{\mathbf{Q}}, i_{x*} i^! R^2 \tilde{\pi}_* \mathbf{Q}_{l,\widetilde{\mathcal{E}}^{(2)}}),$$

where x runs through the closed points of $Z \subset C$ and $i_x : x \to C$ denotes the closed immersion. From the theory of modular curves we see that

$$k(x) := \text{residue field of } x$$

is a subfield of the cyclotomic field $\mathbf{Q}(\zeta_M)$. The fibers of f are also defined over some subfields of $\mathbf{Q}(\zeta_M)$, and hence the same holds for the fibers of $\tilde{\pi}$. That means as $G_{k(x)}$-modules, $i_{x*} i^! R^2 \tilde{\pi}_* \mathbf{Q}_{l,\widetilde{\mathcal{E}}^{(2)}}$ is a direct sum of Abelian characters χ's. The L-function associated to $H^0_{\text{ét}}(x \otimes \overline{\mathbf{Q}}, i_{x*} i^! R^2 \tilde{\pi}_* \mathbf{Q}_{l,\widetilde{\mathcal{E}}^{(2)}})(1)$ is therefore a product of Abelian L-series $L(s, \chi)$. It is classical that at[8] $s = 1$, $L(s, \chi)$ either has a pole or has neither a pole nor a zero; we pick up a pole precisely when $H^0_{\text{ét}}(x \otimes \overline{\mathbf{Q}}, \chi)(1)$ is a 1-dimensional $G_{\mathbf{Q}}$-fixed space of $H^0_{\text{ét}}(x \otimes \overline{\mathbf{Q}}, i_{x*} i^! R^2 \tilde{\pi}_* \mathbf{Q}_{l,\widetilde{\mathcal{E}}^{(2)}})(1)$. Thus the contribution from (44) to the two sides of (42) are equal as well, and the Lemma follows.

□

Remark 14. The Lemma also holds for the universal elliptic curve over $X_1(M)/\mathbf{Q}(\zeta_M)$. This time $H^1(R^1)$ is not empty; but (42) remains true since both sides are still zero. For the analytic side it follows from a deep non-vanishing theorem [8]. For the cohomological side, this follows from the fact that no power of the cyclotomic character is a quotient of the Galois representation associated to a weight 3 cusp forms on $\Gamma_1(M)$.

We now return to Tate's conjecture for $\widetilde{\mathcal{E}}^{(2)}$. As in (25) — (27), we get

$$\begin{aligned} & \frac{d}{ds} \log L_2(\widetilde{\mathcal{E}}^{(2)}/\mathbf{Q}, s) \\ (45) \qquad = \; & 2 \frac{d}{ds} \log L_2(\mathcal{E}/\mathbf{Q}, s) - \sum_p \frac{-\log p}{p^s}(1 + b_2) - \sum_p \frac{-\log p}{p^{s+2}} \sum_{t \in C(\mathbf{F}_p)} a_p(\mathcal{E}_t)^2. \end{aligned}$$

[8] we shift from $s = 2$ to $s = 1$ because of the Tate twist in $H^0_{\text{ét}}(x \otimes \overline{\mathbf{Q}}, i_{x*} i^! R^2 \tilde{\pi}_* \mathbf{Q}_{l,\widetilde{\mathcal{E}}^{(2)}})(1)$

Invoke Theorem 4 and the analytic Tate conjecture just proved for $\mathcal{E}/\mathbf{Q}$, we see that $L_2(\widetilde{\mathcal{E}}^{(2)}/\mathbf{Q}, s)$ has an analytic continuation to $Re(s) > 7/4$ except possibly for a pole at $s = 2$. Moreover, compute the residues on both sides of (45) at $s = 1$ and we get

$$\begin{array}{rcll} \text{rank} NS(\widetilde{\mathcal{E}}^{(2)}/\mathbf{Q}) & \geq & 2\ \text{rank} NS(\mathcal{E}/\mathbf{Q}) + b_2 & \text{by Theorem 3} \\ & = & -\underset{s=2}{\text{ord}}\, L_2(\widetilde{\mathcal{E}}^{(2)}/\mathbf{Q}, s) & \text{by (45)} \\ & \geq & \text{rank} H^2_{\text{ét}}(\mathcal{E} \otimes \overline{\mathbf{Q}}, \mathbf{Q}_l)^{G_{\mathbf{Q}}} & \text{by Lemma 7} \\ & \geq & \text{rank} NS(\widetilde{\mathcal{E}}^{(2)}/\mathbf{Q}) & \end{array}$$

since $NS(\widetilde{\mathcal{E}}^{(2)}/\mathbf{Q}) \otimes \mathbf{Q}_l \hookrightarrow H^2_{\text{ét}}(\mathcal{E} \otimes \overline{\mathbf{Q}}, \mathbf{Q}_l)^{G_{\mathbf{Q}}}$. Thus we have equalities all the way, whence the order of pole at $s = 2$ of $L_2(\widetilde{\mathcal{E}}^{(2)}/\mathbf{Q}, s)$ is $\text{rank} NS(\widetilde{\mathcal{E}}^{(2)}/\mathbf{Q})$, as desired.

□

Remark 15. From this analytic proof of Tate's conjecture for $\widetilde{\mathcal{E}}^{(2)}/\mathbf{Q}$ we see that the inequality in Lemma 7 is in fact an equality. That means

- (41) is in fact an equality, and
- in the notation of the proof of the Lemma, for each $x \in Z$, the $G_{\mathbf{Q}}$-fixed subspace of $H^0_{\text{ét}}(x \otimes \overline{\mathbf{Q}}, i_{x*} i^! R^2 \tilde{\pi}_* \mathbf{Q}_{l, \widetilde{\mathcal{E}}^{(2)}})(1)$ is spanned by precisely to the divisors $A_{ij}(t)$ in (28) for the cusp x plus the blowup divisors.

With a more delicate analysis we should be able to prove these two statements directly. Furthermore, the contribution from the term $H^2(R^0)(1)^{G_{\mathbf{Q}}}$ corresponds to a vertical fiber of $\widetilde{\mathcal{E}_M}^{(2)}$, while the contributions from $H^0_{\text{ét}}(X_0(M) \otimes \overline{\mathbf{Q}}, j_* R^2 \tilde{\pi}_{U*} \mathbf{Q}_{l, \mathcal{E}_U^{(2)}})$ correspond to the divisors $\tilde{E}_1, \tilde{E}_2$ and $\tilde{\Delta}$ in (29). Putting these together and we should get a purely geometric proof — modulo analytic and Galois properties of weight 3 modular forms — of Tate's conjecture for $\widetilde{\mathcal{E}_M}^{(2)}$. We present the analytic argument here because of its own interest, and because it serves as a guide on how to prove Tate's conjecture for $\widetilde{\mathcal{E}}^{(2)}$ for a general semistable fibration $\mathcal{E} \to C$. Specifically, the analytic proof above depends on three ingredients:

- Tate's conjecture for $\mathcal{E}_M$,
- the crucial Lemma 7, and
- the Galois module structure of the bad fibers.

To extend our proof of Lemma 7 to a general semistable fibration $f : \mathcal{E} \to C$, we need to understand the monodromy representation $H^1(R^1)$. This is also the main obstacle to proving Tate's conjecture for $\mathcal{E}$. For the universal elliptic curve over the Fermat curve (cf. Remark 8), we expect the complex multiplication structure of the Fermat curve to greatly facilitate the monodromy computation. In additional, the Galois module structure of the bad fibers of Fermat fibrations is well understood. These issues are currently under investigation.

9. Isotrivial fibrations

Proof of Theorem 6. Let $f : \mathcal{E} \to C$ be a non-split, isotrivial elliptic fibration over $\mathbf{Q}$. Then we can find an integer $n \in \{2, 3, 4, 6\}$, a smooth curve $E/\mathbf{Q}$ of genus one[9] and a non-constant function $g \in \mathbf{Q}(C)$ such that, for all but finite many points $t \in C(\overline{\mathbf{Q}})$, the fiber $f^{-1}(t)$ is the

[9] f is not assumed to have a section, so $E/\mathbf{Q}$ need not be an elliptic curve.

n-th order twist of $E/\mathbf{Q}$ by $g(t)$; in other words, $f^{-1}(t)$ is isomorphic to E over the extension $\mathbf{Q}(t, \sqrt[n]{g(t)})$.

We begin with $n = 2$, i.e. a quadratic twist family. Then $a_p(\mathcal{E}_t) = \pm a_p(E)$ for every smooth fiber $\mathcal{E}_t$, whence by the Weil conjecture,

$$\sum_p \frac{\log p}{p^{s+2}} \sum_{t\in C(\mathbf{F}_p)} a_p(\mathcal{E}_t)^2 \;=\; \sum_p \frac{\log p}{p^{s+1}} a_p(E)^2 + O_{\mathcal{E}}\Big(\sum_p \frac{\log p}{p^{s+3/2}} a_p(E)^2\Big). \tag{46}$$

Note that up to a term that is holomorphic for $Re(s) > 1/2$, the first term on the right side is the logarithmic derivative of the Rankin-Selberg convolution of the L-series of the Jacobian $J_E/\mathbf{Q}$ of $E/\mathbf{Q}$. Since $J_E/\mathbf{Q}$ is a *modular* elliptic curve, the convolution L-series has a simple pole at $s = 0$ and 1 and is holomorphic for $Re(s) > 1$ [10], whence the residue of (46) at $s = 1$ is exactly one. This gives Theorem 6(a) for quadratic twist families.

Next, consider the case $n = 4$. Then $E/\mathbf{Q}$ is a (possibly trivial) $\mathbf{Q}$-torsor of $E_0 : y^2 = x^3 + x$, and $g \in k(C)$ is not a 4-th power. Every smooth curve of genus one over any finite field $\mathbf{F}$ has a $\mathbf{F}$-rational point, so $E/\mathbf{F}_p$ is $\mathbf{F}_p$-isomorphic to $E_D : y^2 = x^3 + D_p x$ for some element $D_p \in \mathbf{F}_p$. Consequently, except for a finite number of $t \in C(\mathbf{F}_p)$ (the number of which is bounded from the above independent of p), $\mathcal{E}_t/p$ is isomorphic to $E_{D_p g(t)}/\mathbf{F}_p$. It is classical [6] that for p sufficiently large,

$$a_p(\mathcal{E}_{D_p g(t)}) = \begin{cases} 0 & \text{if } p \equiv 3 \pmod 4 \\ \chi_p(D_p g(t))^2 a_p(E) & \text{if } p \equiv 1 \pmod 4, \end{cases}$$

where for $p \equiv 1 \pmod 4$, $\chi_p : (\mathbf{Z}/p)^\times \to \mathbf{C}$ is a character of order 4. Consequently,

$$\sum_p \frac{\log p}{p^{s+2}} \sum_{t\in C(\mathbf{F}_p)} a_p(\mathcal{E}_t)^2 \;=\; \Big(\sum_{p\equiv 3(4)} \frac{\log p}{p^{s+2}} a_p(E)^2\Big) \cdot O_{\mathcal{E}}(1) + \tag{47}$$

$$\sum_{p\equiv 1(4)} \frac{\log p}{p^{s+2}} a_p(E)^2 \chi_p(D_p)^2 \sum_{t\in C(\mathbf{F}_p)} \chi_p(g(t))^2. \tag{48}$$

Denote by $C'/\mathbf{F}_p$ the double cover of C given by the (possibly singular) model $z^2 = g(t)$. Then the inner sum in (48) is simply

$$\sum_{t'\in C'(\mathbf{F}_p)} a_p(C') + O_{\mathcal{E}}(1),$$

where the O-constant is independent of p. This is $O_{\mathcal{E}}(\sqrt{p})$ by the Weil conjecture, so the residue at $s = 1$ of the left side of (47) is zero. The same argument applies *mutatis mutandis* to the case $n = 3$ and $n = 6$.

□

Remark 16. In order to apply this argument to general isotrivial surfaces over a number field, we need to understand the analytic properties for the convolution of L-series of elliptic curves over number fields. That seems to be a very difficult problem.

Using known results on symmetric third- and fourth-powers L-functions, we can extend the argument above to a_p^3- and a_p^4-sums of isotrivial fibrations over $\mathbf{Q}$. Higher a_p-powers are beyond current techniques.

Acknowledgement

I am grateful to the support and encouragement of Barry Mazur, Michael Rosen and Joe Silverman, over the years and for this project in particular. David Cox offers excellent tutorials on toric geometry. Dan Abramovich patiently explains to me the fine points of Cartier divisors. Peter Sarnak draws our attention to the work of Birch and suggests that it could be related to the a_p^n-Nagao sums. Brian Conrad and Eyal Markman patiently answer many of my questions. My thanks to all of them. Any error that remains is due to me.

References

[1] B. J. Birch, How the number of points of an elliptic curve over a fixed prime field varies. *J. London Math. Soc.* **43** (1968) 57-60.

[2] S. Bosch, W. Lütkebohmert and M. Raynaud, *Néron models.* Springer-Verlag, 1990.

[3] P. Deligne, Formes modulaires et représentations l-adiques, in: *Séminaire Bourbaki.* 1968/69, exp. 355.

[4] D. Eisenbud and J. Harris, *The geometry of schemes.* Springer-Verlag, 2000.

[5] B. Gordon, Algebraic cycles and the Hodge structure of a Kuga fiber variety. *Trans. AMS* **336** (1993) 933-947.

[6] K. Ireland and M. Rosen, *A classical introduction to modern number theory.* Second edition. Springer-Verlag, 1990

[7] H. Ito, On the number of rational cyclic subgroups of elliptic curves over finite fields. *Mem. College Ed. Akita Univ. Natur. Sci.* No. 41 (1990) 33-42.

[8] H. Jacquet and J. A. Shalika, A non-vanishing theorem for zeta functions of GL_n. *Invent. Math.* **38** (1976/77) 1-16.

[9] S. Lang, *Fundamentals of Diophantine geometry.* Springer-Verlag, 1983.

[10] W. Li, L-series of Rankin type and their functional equations. *Math. Ann.* **244** (1979) 135-166.

[11] S. Lichtenbaum, Curves over discrete valuation rings. *Amer. J. Math.* **90** (1968) 380-404.

[12] J. F. Mestre, Construction d'une courbe elliptique de rank $\geq$ 12. C. R. Acad. Sci. Paris, Ser. I, **295** (1982) 643-644.

[13] K. Nagao, Construction of high-rank elliptic curves. *Kobe J. Math.* **11** (1994) 211-219.

[14] K. Nagao, $\mathbf{Q}(T)$-rank of elliptic curves and certain limits coming from the local points. *Manuscripta Math.* **92** (1997) 13-32.

[15] A. P. Ogg, Diophantine equations and modular forms. *Bull. A.M.S.* **81** (1975) 14-27.

[16] M. Rosen and J. Silverman, On the rank of an elliptic surface. *Invent. Math.* **133** (1998) 43-67.

[17] M. Saito and K. Sakakibara, On Mordell-Weil lattices of higher genus fibrations on rational surfaces. *J. Math. Kyoto Univ.* **34** (1994) 859-871.

[18] C. Schoen, Complex multiplication cycles on elliptic modular threefolds. *Duke Math. J.* **53** (1986) 771-794.

[19] T. Scholl, Motives for modular forms. *Invent. Math.* **100** (1990) 419-430.

[20] R. Schoof, Nonsingular plane cubic curves over finite fields. *J. Combin. Theory Ser. A* **43** (1987) 183-211.

[21] R. Schoof and M. van der Vlugt, Hecke operators and the weight distributions of certain codes. *J. Combin. Theory Ser. A* **57** (1991) 163-186.

[22] T. Shioda, On elliptic modular surfaces. *J. Math. Soc. Japan* **24** (1972) 1-59.

[23] T. Shioda, Frey's elliptic curve as an elliptic surface over the Fermat curve. *Comment. Math. Univ. St. Paul* **38** (1989) 223-232.

[24] T. Shioda, On the Mordell-Weil lattice. *Comm. Math. Univ. St. Pauli* **39** (1990) 211-240.

[25] T. Shioda, Generalization of a Theorem of Manin-Shafarevich. *Proc. Japan Acad.* **69A** (1993) 10-12.

[26] T. Shioda, Mordell-Weil lattice for higher genus fibration over a curve, in: *New Trends in Algebraic Geometry*, 359-373. Cambridge Univ. Press, 1999.

[27] J. Tate, Algebraic cycles and the pole of zeta functions, in: *Arithmetical algebraic geometry.* Harper and Row, New York (1965), 93-110.

[28] J. Tate, On the conjectures of Birch and Swinnerton-Dyer and a geometric analog, in: *Séminaire Bourbaki* **9** 1964/65-1965/66, exp. 306.

[29] W. C. Waterhouse, Abelian varieties over finite fields. *Ann. Sci. Éc. Norm. Sup.* **4** (1969) 521-560.
[30] R. Wazir, *Arithmetic on elliptic threefolds.* Ph. D. dissertation. Brown University, May 2001.

Department of Mathematics, University of Massachusetts. Amherst, MA 01003-4515
E-mail address: simanⓜmath.umass.edu